L.YA. KULIKOV

ALGÈBRE ET THÉORIE DES NOMBRES

L. KOULIKOV

ALGÈBRE
ET THÉORIE DES NOMBRES

ÉDITIONS MIR · MOSCOU

AVANT-PROPOS

Ces dernières années on a introduit dans les instituts pédagogiques un nouveau programme de cours unifié d'algèbre et de théorie des nombres. L'objet principal de ce cours est l'étude des systèmes algébriques fondamentaux ainsi que la formation de la culture algébrique des futurs enseignants nécessaire à la compréhension profonde des objectifs et des tâches d'un cours scolaire des mathématiques élémentaires ou à option. L'ouvrage proposé a été rédigé en se conformant aux nouveaux programmes.

Conventionnellement l'ouvrage peut être divisé en trois parties liées intimement entre elles. La première partie présente des éléments de logique, des concepts concernant les ensembles et les relations, des notions préliminaires sur les algèbres et les systèmes algébriques, les systèmes numériques de base. Les éléments de logique et de théorie des ensembles sont exposés de façon suffisamment complète et sont, ensuite, largement utilisés dans le cours d'algèbre et autres branches des mathématiques. L'information préliminaire sur les algèbres et les systèmes algébriques, les groupes et les anneaux est fournie par le chapitre III. Sur cette base sont étudiés les systèmes numériques fondamentaux: système des nombres naturels, anneau des entiers, corps des nombres rationnels, système des nombres réels et corps des nombres complexes. Le système des nombres réels est introduit comme un corps complet totalement ordonné (archimédien). La seconde partie (chapitres V-IX) est réservée à l'algèbre linéaire. On étudie d'abord les espaces vectoriels arithmétiques et les systèmes d'équations linéaires, abstraction faite des déterminants. C'est seulement au chapitre VI que les déterminants sont appliqués à la résolution des systèmes d'équations linéaires. Cette manière de procéder non traditionnelle allège le calcul des principaux problèmes, la théorie des systèmes d'équations linéaires s'incorporant ainsi organiquement à la théorie des espaces vectoriels arithmétiques. Le chapitre IX traite des systèmes d'inégalités linéaires et des éléments de programmation linéaire (problèmes canoniques et problèmes standards, principe de dualité et méthode du simplexe).

La troisième partie du livre (chapitres X-XVII) est réservée aux groupes, aux sujets numériques théoriques, aux anneaux et aux anneaux des polynômes. Dans les deux derniers chapitres on étudie les anneaux des polynômes associés aux corps numériques de base ainsi que les éléments de la théorie des corps.

Plusieurs chapitres sont étroitement liés aux nouveaux programmes scolaires et peuvent servir de base aux cours scolaires à option.

Tous les chapitres sont divisés en paragraphes. Si l'on se réfère au paragraphe du chapitre, on n'indique que le numéro du paragraphe. Dans la référence au paragraphe d'un autre chapitre le numéro du chapitre précède celui du paragraphe cité. Les théorèmes, les propositions et les corollaires d'un même paragraphe sont numérotés successivement. La référence au théorème ou à la proposition du chapitre est faite en indiquant le numéro du paragraphe suivi de celui du théorème. La référence au théorème ou à la proposition d'un autre chapitre comporte successivement le numéro du chapitre, du paragraphe et du théorème. Par exemple, la référence « théorème 4.2 » signifie théorème 2 du paragraphe 4 du même chapitre, « théorème 4.2.6 », théorème 6 du paragraphe 2 du chapitre IV.

L'auteur remercie chaleureusement les professeurs B.M. Brédikhine et M.M. Gloukhov pour leurs analyses et remarques critiques ayant permis d'améliorer le manuscrit du livre.

Auteur

CHAPITRE PREMIER

ÉLÉMENTS DE LOGIQUE

§ 1. Logique des assertions

Assertions. La notion d'« assertion » est primaire. On entend en logique par assertion l'énoncé d'une proposition dont on peut dire qu'elle est vraie ou bien fausse. Toute assertion est soit vraie soit fausse et aucune assertion ne peut être à la fois vraie et fausse.

Exemples d'assertions: « $0 < 1$ », « $2 \cdot 3 = 6$ », « 5 est un nombre pair », « 1 est un nombre premier ». La valeur de vérité des deux premières assertions est « vrai », la valeur de vérité des deux dernières est « faux ».

Les propositions interrogatives et exclamatives ne sont pas des assertions. Une définition n'est pas une assertion. Par exemple, la définition « un nombre entier est dit pair s'il est divisible par 2 » n'est pas une assertion. Or, l'énoncé de la proposition « si un nombre entier est divisible par 2 il est alors pair » constitue une assertion qui, de plus, est vraie. La logique des assertions fait abstraction du sens logique de l'assertion et se contente de répondre sans ambiguïté à la question: la proposition énoncée est-elle vraie ou fausse?

Dans la suite de l'exposé on entendra par sens de l'assertion sa valeur de vérité (l'assertion est-elle « vraie » ou « fausse »?). Les assertions seront notées par des capitales latines, tandis que leurs valeurs, c'est-à-dire le fait qu'elles sont vraies ou fausses, respectivement par les lettres V et F.

La logique des assertions étudie les relations qui se déterminent de façon exhaustive par les procédés permettant de former d'autres assertions à partir d'assertions dites *élémentaires*. Les assertions élémentaires sont considérées comme entières, indivisibles en parties; leur structure interne ne nous intéressera pas.

Opérations logiques sur les assertions. A partir d'assertions élémentaires, au moyen d'opérations logiques, on peut obtenir des assertions nouvelles, plus compliquées. La valeur de vérité de l'assertion complexe est fonction des valeurs de vérité d'assertions formant l'assertion complexe. Cette dépendance s'établit au moyen des définitions données plus loin et peut être constatée en construisant les tables de vérité. Dans les colonnes de gauche de ces tables sont indiquées les dispositions possibles des valeurs de

vérité d'assertions formant l'assertion complexe considérée. Dans la colonne de droite on inscrit les valeurs de vérité de l'assertion complexe correspondant aux distributions de chaque ligne.

Soient A et B deux assertions quelconques sur les valeurs de vérité desquelles on s'abstient de faire des hypothèses. On appelle *négation de l'assertion* A la nouvelle assertion vraie si et seulement si A est faux. La négation A est notée $\neg A$ et est lue « non A » ou « négation de A ». L'opération de négation se définit complètement par la table de vérité

A	$\neg A$
V	F
F	V

.

E x e m p l e. L'assertion « il est faux que 5 est un nombre pair », dont la valeur est V, est la négation de la fausse assertion « 5 est un nombre pair ».

A l'aide de l'opération de *conjonction* on forme à partir de deux assertions une assertion complexe notée $A \wedge B$. Par définition, l'assertion $A \wedge B$ est vraie si et seulement si les deux assertions A et B sont vraies. Les assertions A et B sont respectivement appelées *premier* et *second membres de la conjonction* $A \wedge B$. La notation « $A \wedge B$ » se lit « A et B ». La table de vérité de la conjonction est de la forme

A	B	$A \wedge B$
V	V	V
V	F	F
F	V	F
F	F	F

E x e m p l e. L'assertion « 7 est un nombre premier et 6 un nombre impair » est fausse, comme conjonction de deux assertions dont l'une est fausse.

On appelle *disjonction* de deux assertions A et B l'assertion notée $A \vee B$, vraie si et seulement si une seule des assertions A et B est vraie. Respectivement, l'assertion $A \vee B$ est fausse si et seulement si A et B sont tous les deux faux. Les assertions A et B sont de même appelées *premier* et *second membres de la disjonction* $A \vee B$. On lit la notation $A \vee B$ « A ou bien B ». La conjonction « ou » a dans ce cas un sens non exclusif, puisque l'assertion $A \vee B$ est vraie si les deux membres sont vrais. La disjonction peut se présenter sous forme de table de vérité suivante :

A	B	$A \vee B$
V	V	V
V	F	V
F	V	V
F	F	F

E x e m p l e. L'assertion « $3 < 8$ ou $5 < 2$ » est une disjonction de deux assertions dont l'une est vraie, sa valeur est V.

L'assertion notée $A \to B$, fausse si et seulement si A est vrai, tandis que B est faux, est appelée *implication* avec prémisse A et conclusion B. L'assertion $A \to B$ se lit « si A, alors B » ou bien « A implique B », ou encore « de A s'ensuit B ». La table de vérité de l'implication est de la forme

A	B	$A \to B$
V	V	V
V	F	F
F	V	V
F	F	V

Remarquons qu'entre la prémisse et la conclusion il peut ne pas exister de relation de cause à effet, toutefois, ce fait n'entérine pas la vérité ou la fausseté de l'implication. Par exemple, l'assertion « si 5 est un nombre premier, la bissectrice d'un triangle isocèle est une médiane » est vraie bien que selon le sens commun la seconde assertion ne découle pas de la première. Sera également vraie l'assertion « si $2 + 2 = 5$, alors $6 + 3 = 9$ », car sa conclusion est vraie. Avec cette définition si la conclusion est vraie, l'implication sera vraie quelle que soit la valeur de vérité de la prémisse. Au cas où la prémisse est fausse, l'implication sera vraie indépendamment de la valeur de vérité de la conclusion. Cette circonstance s'énonce sommairement ainsi : « la vérité peut provenir de tout », « tout peut provenir d'une assertion fausse ».

L'assertion notée $A \leftrightarrow B$, vraie si et seulement si A et B ont la même valeur de vérité, est appelée *équivalence*. L'assertion $A \leftrightarrow B$ se lit « A si et seulement si B » ou « A est équivalent à B » ou encore « A est une condition nécessaire et suffisante pour que B ait lieu ». La table de vérité pour l'équivalence est de la forme

A	B	$A \leftrightarrow B$
V	V	V
V	F	F
F	V	F
F	F	V

E x e m p l e. L'assertion « $2 > 5$ si et seulement si $3 + 0 = 4$ » est vraie comme une équivalence de deux assertions fausses.

Formules de la logique des assertions. L'objectif principal de la l o g i q u e d e s a s s e r t i o n s est l'étude des formes logiques des assertions complexes au moyen d'opérations logiques. La notion de forme logique de l'assertion complexe s'éclaircie par l'introduction de la notion de formule de la logique des assertions faite plus loin.

Pour la notation d'assertions on utilisera les minuscules latines

de la fin de l'alphabet (si besoin avec indices). Par hypothèse on ignore dans ce cas quelle assertion (vraie ou fausse) est désignée par telle ou telle lettre. En fait les lettres

(1) $p, q, r, \ldots, p_1, q_1, r_1, \ldots$

seront des variables acquérant en guise de valeurs les valeurs de vérité « vrai » et « faux ». Généralement, ces variables sont appelées *variables propositionnelles*; on les appellera également *formules élémentaires* ou *atomes*.

Pour les formules de la logique des assertions on utilise outre les symboles (1) des signes d'opérations logiques

$\neg, \wedge, \vee, \rightarrow, \leftrightarrow,$

de même que des symboles garantissant une lecture univalente des formules — parenthèses gauche et droite: (,).

Présentons la notion de *formule de la logique des assertions* de la façon suivante:

1) les formules élémentaires (les atomes) constituent des formules de la logique des assertions;

2) si A et B sont des formules, $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$ sont également des formules de la logique des assertions;

3) seules les expressions constituant des inférences de 1) et 2) sont des formules de la logique des assertions.

La définition de la formule implique l'énumération des règles de composition des formules. Selon la définition toute formule de la logique des assertions est soit un atome, soit une expression formée d'atomes et obtenue par application suivie de la règle 2). Par exemple, les expressions

$p, \quad (\neg q), \quad ((r \vee s) \rightarrow t), \quad ((p \vee (\neg p)) \leftrightarrow (p \rightarrow q))$

sont des formules de la logique des assertions.

On notera les formules arbitraires de la logique des assertions au moyen des capitales latines (affectées si nécessaire d'indices):

$A, B, C, \ldots, A_1, B_1, C_1, \ldots$

Il n'est de même pas exclu qu'une même formule puisse être exprimée par des lettres différentes.

Notons qu'aucun atome ne peut se présenter sous la forme $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$. C'est l'aspect que peuvent acquérir des formules complexes.

Dans le chapitre premier au lieu de « formule de la logique des assertions » on dira tout simplement « formule » là où cela n'entraînera aucune équivoque.

Le nombre de parenthèses peut être réduit en posant la convention : 1) dans une formule complexe on supprimera les deux parenthèses extérieures; 2) on ordonne les signes d'opérations logiques

suivant un ordre de priorité donné: $\leftrightarrow$, $\rightarrow$, $\vee$, $\wedge$, $\neg$. Dans cette suite de signes, le signe $\leftrightarrow$ a le domaine d'action le plus large, et le signe $\neg$, le plus restreint. On entend par domaine d'action du signe d'opération les parties de la formule auxquelles s'« applique » (sur lesquelles « agit ») le signe introduit considéré. On convient de ne pas entourer de parenthèses les parties des formules qui peuvent être lues compte tenu de la hiérarchie de la force liante. En restituant les parenthèses on encadre d'abord les parties qui portent le signe $\neg$ (en allant de gauche à droite), ensuite les parties qui portent le signe $\wedge$, etc.

Exemple. Dans la formule $B \leftrightarrow \neg C \vee D \wedge A$ les parenthèses se restituent par étapes de la façon suivante:

$$B \leftrightarrow (\neg C) \vee D \wedge A, \qquad B \leftrightarrow ((\neg C) \vee (D \wedge A)),$$
$$B \leftrightarrow (\neg C) \vee (D \wedge A), \quad (B \leftrightarrow ((\neg C) \vee (D \wedge A))).$$

On ne peut s'abstenir de parenthèses dans toute formule. Par exemple, dans les formules $A \rightarrow (B \rightarrow C)$, $\neg(A \rightarrow B)$ il est impossible de procéder à une subséquente élimination des parenthèses.

Lois logiques. Il existe des formules qui demeurent valables (sont vraies) indépendamment des valeurs du contenu des atomes qui les forment. Par exemple,

$$A \vee \neg A, \quad A \rightarrow A, \quad (A \rightarrow B) \vee (B \rightarrow A), \quad A \rightarrow (B \rightarrow A).$$

Ces formules jouent un rôle particulier en logique.

DÉFINITION. Une formule de la logique des assertions qui acquiert la valeur « vrai » pour toute distribution des valeurs atomiques constituant la formule est dite *toujours vraie*, *tautologie* ou *loi logique*.

Il existe des formules non valables (c'est-à-dire fausses) quelles que soient les valeurs des atomes constituants. Par exemple,

$$A \wedge \neg A, \quad (A \vee \neg A) \rightarrow (A \wedge \neg A).$$

DÉFINITION. Une formule de la logique des assertions qui reste fausse pour toute distribution des valeurs atomiques constituant la formule est dite *toujours fausse* ou *contradiction*.

Il est facile de se convaincre que si A est une contradiction, $\neg A$ sera une tautologie et inversement. Par exemple, la formule $p \wedge \neg p$ est toujours fausse, tandis que $\neg (p \wedge \neg p)$ est une tautologie.

Il existe des formules qui prennent soit la valeur « vrai », soit la valeur « faux » suivant les valeurs qu'acquièrent les atomes qui y figurent. Par exemple,

$$A \vee A, \quad A \rightarrow B, \quad A \wedge B \rightarrow B \wedge C.$$

La notation $\models A$ signifie que A est une tautologie; par exemple, $\models A \vee \neg A$. Cette loi porte le nom de *loi du tiers exclu*.

THÉORÈME 1.1. *Si A et $(A \rightarrow B)$ sont des tautologies, B est aussi une tautologie.*

D é m o n s t r a t i o n. Supposons que A et $(A \to B)$ sont des tautologies. Admettons que pour une distribution quelconque des valeurs de vérité des atomes formant A et B la formule B prenne la valeur « faux ». Vu que A est une tautologie, pour une même distribution des valeurs de vérité des atomes, la formule A acquiert la valeur « vrai ». Par suite, la formule $(A \to B)$ est donc fausse, ce qui est contraire à l'hypothèse selon laquelle $(A \to B)$ est une tautologie. Par conséquent, la formule B est V pour toute distribution des valeurs de vérité de ses atomes. □ *)

THÉORÈME 1.2. *Soit A une formule contenant des atomes $p_1, \ldots, p_n$, tandis que B est une formule qu'on obtient à partir de A en substituant en même temps à $p_1, \ldots, p_n$ les formules $A_1, \ldots, A_n$ respectivement. Si A est une tautologie, B l'est aussi.*

D é m o n s t r a t i o n. Supposons donnée une distribution quelconque des valeurs de vérité des atomes composant B. Pour cette distribution des valeurs des atomes les formules $A_1, \ldots, A_n$ prendront respectivement les valeurs de vérité $a_1, \ldots, a_n$. Si on donne aux atomes $p_1, \ldots, p_n$ respectivement les valeurs $a_1, \ldots, a_n$ la valeur de vérité de la formule A coïncidera alors avec celle de la formule B pour la distribution donnée des valeurs des atomes formant B. Vu que par hypothèse A est une tautologie, pour la distribution donnée des valeurs des atomes B a la valeur « vrai », c'est-à-dire B est aussi une tautologie. □

Ce théorème montre que toute permutation dans une tautologie conduit à une tautologie.

On donne plus bas (avec le théorème 1.3) les lois logiques les plus fréquentes.

THÉORÈME 1.3. *Les formules suivantes sont des tautologies:*

Implications tautologiques:

$p \wedge (p \to q) \to q$	*loi de conclusion;*
$\left.\begin{array}{l} p \wedge q \to p \\ p \wedge q \to q \end{array}\right\}$	*lois d'élimination de la conjonction;*
$\left.\begin{array}{l} p \to p \vee q \\ q \to p \vee q \end{array}\right\}$	*lois d'inclusion de la disjonction;*
$(p \vee q) \wedge \neg q \to p$	*loi d'élimination de la disjonction;*
$p \to \neg\neg p$	*loi d'inclusion de la double négation;*
$\neg\neg p \to p$	*loi d'élimination de la double négation;*

*) Le signe □ signifie que la démonstration du théorème ou de la proposition est achevée.

$(p \to q) \wedge (q \to p) \to (p \leftrightarrow q)$	*loi d'inclusion de l'équivalence* ;
$\left.\begin{array}{l}(p \leftrightarrow q) \to (p \to q)\\(p \leftrightarrow q) \to (q \to p)\end{array}\right\}$	*lois d'élimination de l'équivalence* ;
$(p \to q) \to (\neg q \to \neg p)$	*loi de contraposition* ;
$(\neg p \to q) \wedge (\neg p \to \neg q) \to p$	*loi de démonstration a contrario* ;
$(p \to q) \wedge (q \to r) \to (p \to r)$	*loi du syllogisme* ;
$(p \to r) \wedge (q \to r) \to (p \vee q \to r)$	*loi d'addition des prémisses* ;
$(p \to q) \wedge (p \to r) \to (p \to q \wedge r)$	*loi du produit des conclusions* ;
$(p \leftrightarrow q) \wedge (q \leftrightarrow r) \to (p \leftrightarrow r)$	*loi de la transitivité de l'équivalence*.

Equivalences tautologiques :

$p \leftrightarrow p$	*loi d'identité* (*d'équivalence logique*) ;
$p \wedge p \leftrightarrow p$	*loi de l'idempotence de la conjonction* ;
$p \vee p \leftrightarrow p$	*loi de l'idempotence de la disjonction* ;
$p \wedge q \leftrightarrow q \wedge p$	*loi de la commutativité de la conjonction* ;
$p \vee q \leftrightarrow q \vee p$	*loi de la commutativité de la disjonction* ;
$p \wedge (p \wedge r) \leftrightarrow (p \wedge q) \wedge r$	*loi de l'associativité de la conjonction* ;
$p \vee (q \vee r) \leftrightarrow (p \vee q) \vee r$	*loi de l'associativité de la disjonction* ;
$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$	*loi de la distributivité de la conjonction relativement à la disjonction* ;
$p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$	*loi de la distributivité de la disjonction relativement à la conjonction* ;
$\neg\neg p \leftrightarrow p$	*loi de la double négation* ;
$(p \leftrightarrow q) \leftrightarrow (q \leftrightarrow p)$	*loi de la commutativité de l'équivalence* ;
$(p \to q) \leftrightarrow (\neg q \to \neg p)$	*loi de contraposition* ;
$\neg (p \vee q) \leftrightarrow (\neg p \wedge \neg q)$	*loi de négation de la disjonction* ;
$\neg (p \wedge q) \leftrightarrow (\neg p \vee \neg q)$	*loi de négation de la conjonction* ;

$(p \leftrightarrow q) \leftrightarrow (\neg p \leftrightarrow \neg q)$ *loi des contraires ;*

$p \rightarrow (q \rightarrow r) \leftrightarrow q \rightarrow (p \rightarrow r)$ *loi de permutation des prémisses.*

Tautologies traduisant certaines opérations au moyen d'autres opérations :

$p \rightarrow q \leftrightarrow \neg p \vee q$;

$p \rightarrow q \leftrightarrow \neg (p \wedge \neg q)$;

$p \vee q \leftrightarrow \neg p \rightarrow q$;

$p \vee q \leftrightarrow \neg (\neg p \wedge \neg q)$;

$p \wedge q \leftrightarrow \neg (p \rightarrow \neg q)$;

$p \wedge q \leftrightarrow \neg (\neg p \vee \neg q)$;

$(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$.

Pour démontrer que chacune des formules fournies est une tautologie il faut recourir à la méthode des tables de vérité, c'est-à-dire construire pour chaque formule la table de vérité et s'assurer que sur chaque ligne de la colonne marginale de droite figure la lettre V.

A titre d'exemple prenons la loi du syllogisme :

p	q	r	$p \rightarrow q$	$q \rightarrow r$	$p \rightarrow r$	$(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$
V	V	V	V	V	V	V
V	V	F	V	F	F	V
V	F	V	F	V	V	V
V	F	F	F	V	F	V
F	V	V	V	V	V	V
F	V	F	V	F	V	V
F	F	V	V	V	V	V
F	F	F	V	V	V	V

Notons qu'en vertu des lois d'associativité il est possible de supprimer les parenthèses encadrant le groupe de membres formés de conjonctions et disjonctions polynomiales. A partir de la loi de la double négation il découle, si besoin est, qu'une suite successive de deux signes « $\neg$ » ou plus est toujours évitable.

Exercices

1. Construire la table de vérité pour chacune des formules

(a) $p \rightarrow q \leftrightarrow \neg p \vee q$; (c) $r \rightarrow (r \rightarrow q)$;

(b) $p \rightarrow \neg (q \wedge r)$; (d) $(p \wedge q) \rightarrow (s \wedge \neg s \rightarrow p \vee s)$.

2. Que peut-on dire de la valeur « vrai » de l'assertion $\neg A \wedge B \leftrightarrow A \vee B$ si la valeur de l'assertion $A \rightarrow B$ est qualifiée « faux »?

3. Démontrer que les formules du théorème 1.3 sont des tautologies.

4. Soit C une formule impliquant une inclusion de la formule A, tandis que C' est la formule obtenue à partir de C en remplaçant cette inclusion de la formule A par la formule B. Démontrer que si $A \leftrightarrow B$ est une tautologie, $C \leftrightarrow C'$ l'est également.

5. Combien de lignes possède la table de vérité de la formule logique d'assertions formée de n atomes différents?

6. Supposons que la formule A est construite à partir des atomes $p_1, \ldots, p_n$ uniquement à l'aide des signes $\neg$, $\wedge$, $\vee$, et la formule A^* est obtenue à partir de A en remplaçant chaque inclusion de $\wedge$ par le symbole $\vee$ et inversement; et, en remplaçant chaque inclusion p_i par l'inclusion $\neg p_i$ et inversement. Démontrer que la formule $\neg A \leftrightarrow A^*$ est une tautologie.

7. Démontrer que les formules suivantes sont des tautologies:

(a) $(A \wedge B) \to C \leftrightarrow A \to (B \to C)$;
(b) $(A \wedge B) \to C \leftrightarrow (A \wedge \neg C) \to \neg B$;
(c) $\neg (A \to B) \leftrightarrow A \wedge \neg B$;
(d) $(A \to B) \wedge \neg B \to \neg A$;
(e) $A \to (\neg A \to B)$;
(f) $A \to (B \to A)$;
(g) $(\neg A \to A) \to A$;
(h) $(A \to B) \to (A \wedge C \to B \wedge C)$;
(i) $(A \to B) \wedge (C \to D) \to (A \wedge C \to B \wedge D)$;
(k) $(A \to B) \wedge (C \to D) \to (A \vee C \to B \vee D)$;
(l) $\neg(A \leftrightarrow B) \leftrightarrow (\neg(A \to B) \vee \neg(B \to A))$.

8. Montrer qu'aucune formule de la logique des assertions construite uniquement avec les signes d'opérations logiques $\wedge$, $\vee$ ne constitue ni une tautologie, ni une contradiction.

§ 2. Déduction logique

Définitions principales. Soient $A_1, \ldots, A_m, B$ les formules de la logique des assertions.

DÉFINITION. La formule B est appelée *déduction logique des formules* $A_1, \ldots, A_m$ si avec un choix quelconque des valeurs de vérité des atomes, entrant dans les formules $A_1, \ldots, A_m, B$, la formule B acquiert la valeur « vrai » chaque fois où chacune des formules $A_1, \ldots, A_m$ est vraie.

La notation

$$A_1, \ldots, A_m \models B$$

signifie que la formule B est la déduction logique des formules $A_1, \ldots, A_m$ ($A_1, \ldots, A_m$ entraînant logiquement B).

En recourant aux tables de vérité on dira que la formule B est la déduction logique des formules $A_1, \ldots, A_m$ si dans les tables construites suivant la suite des atomes $p_1, \ldots, p_n$, entrant dans $A_1, \ldots, A_m, B$, la formule B possède la valeur « vrai » sur toutes les lignes où, simultanément, $A_1, \ldots, A_m$ prennent la valeur « vrai ». Autrement dit, la collection des jeux de valeurs d'atomes pour les-

quels toutes les formules $A_1, \ldots, A_m$ sont vraies appartient à la collection des jeux de valeurs d'atomes pour lesquels la formule B est vraie. La suite d'atomes $p_1, \ldots, p_n$, entrant dans les formules $A_1, \ldots, A_m, B$, peut apparemment acquérir un ordre quelconque.

Exemple. $A \to B,\ A \to \neg B \models \neg A$, ce qui s'ensuit de la table:

A	B	$A \to B$	$A \to \neg B$	$\neg A$
V	V	V	F	F
V	F	F	V	F
F	V	V	V	V
F	F	V	V	V

A partir de la définition de la déduction logique il découle que la tautologie s'ensuit logiquement de toute formule de la logique des assertions, tandis que la contradiction infère toute formule.

DÉFINITION. Les formules A et B sont dites *équipotentes* (*logiquement équivalentes*) si pour un choix quelconque des valeurs de vérité d'atomes, entrant dans A et B, les formules A et B prennent des valeurs de vérité identiques.

La notation $A \equiv B$ signifie que les formules A et B sont équipotentes.

De la définition de l'équivalence logique des formules il découle que toutes deux tautologies sont logiquement équivalentes de même que deux contradictions quelconques.

La formule A *est équipotente à* B *si et seulement si* $A \models B$ *et* $B \models A$.

THÉORÈME 2.1. *Les formules A et B sont équipotentes si et seulement si la formule* $A \leftrightarrow B$ *est une tautologie.*

On propose au lecteur d'esquisser la démonstration en guise d'exercice.

THÉORÈME 2.2. (a) $A \models B$ *si et seulement si* $\models A \to B$; (b) $A_1, \ldots, A_m \models B$ *si et seulement si* $\models A_1 \wedge \ldots \wedge A_m \to B$.

Démonstration. (a) Soit $A \models B$. L'implication $A \to B$ a la valeur de vérité F si A est « vrai » avec, simultanément, B « faux ». Or, en vertu de $A \models B$ posé, il ne peut exister de telle distribution de valeurs de vérité pour les atomes entrant dans A et B. Par conséquent, la formule $A \to B$ acquiert toujours la valeur V, c'est-à-dire $\models A \to B$.

Posons maintenant que $\models A \to B$. Voyons la distribution quelconque des valeurs de vérité des atomes entrant dans A et B pour laquelle A est vrai. Comme par hypothèse avec cette distribution $A \to B$ est qualifié V, B acquiert, cette distributivité se conservant, la valeur V. Donc, $A \models B$.

(b) A partir de la définition de la conjonction on a $A_1, \ldots, A_m \models B$ si et seulement si $A_1 \wedge \ldots \wedge A_m \models B$. En outre, en vertu

de (a),

$$A_1 \wedge \ldots \wedge A_m \models B \text{ si et seulement si } \models A_1 \wedge \ldots \wedge A_m \rightarrow B.$$

Par conséquent, $A_1, \ldots, A_m \models B$ si et seulement si $\models A_1 \wedge \ldots \wedge A_m \rightarrow B$. □

Exemple. $(A \rightarrow B), (B \rightarrow C) \models (A \rightarrow C)$, vu que la formule $(A \rightarrow B) \wedge (B \rightarrow C) \rightarrow (A \rightarrow C)$ est une tautologie.

THÉORÈME 2.3. *$A_1, \ldots, A_m, B \models C$ si et seulement si $A_1, \ldots, A_m \models B \rightarrow C$.*

Démonstration. Supposons que $A_1, \ldots, A_m, B \models C$ et montrons alors que $A_1, \ldots, A_m \models B \rightarrow C$. Admettons qu'il existe une distribution des valeurs de vérité des atomes entrant dans les formules $A_1, \ldots, A_m, B, C$ pour laquelle les formules $A_1, \ldots, A_m$ ont pour valeur V, tandis que la formule $B \rightarrow C$ est F. Pour cette même distribution des valeurs d'atomes les formules $A_1, \ldots, A_m, B$ prendraient simultanément la valeur V, tandis que la formule C serait fausse. Donc, il n'existe pas de telle distribution des valeurs de vérité d'atomes. Par suite, si $A_1, \ldots, A_m, B \models C$, on a $A_1, \ldots, A_m \models B \rightarrow C$.

Supposons maintenant que $A_1, \ldots, A_m \models B \rightarrow C$ et montrons que $A_1, \ldots, A_m, B \models C$. Admettons qu'il existe une distribution des valeurs de vérité d'atomes entrant dans les formules $A_1, \ldots, A_m, B, C$ pour laquelle les formules $A_1, \ldots, A_m, B$ ont la valeur V, tandis que les formules C sont fausses. Avec une distribution identique des valeurs de vérité d'atomes les formules $A_1, \ldots, A_m$ prendraient la valeur V et la formule $B \rightarrow C$ la valeur F, ce qui est en contradiction avec l'hypothèse. Par conséquent, il n'existe pas de telle distribution de valeurs de vérité pour les atomes. Par suite, si $A_1, \ldots, A_m \models B \rightarrow C$, on a $A_1, \ldots, A_m, B \models C$. □

COROLLAIRE 2.4. *$A, B \models C$ si et seulement si $\models A \rightarrow (B \rightarrow C)$. Sous une forme plus générale: $A_1, A_2, \ldots, A_m \models B$ si et seulement si $\models A_1 \rightarrow (A_2 \rightarrow (\ldots (A_m \rightarrow B) \ldots))$.*

Pour esquisser la démonstration il suffit d'appliquer plusieurs fois le théorème 2.3.

Il s'ensuit du théorème 2.3 qu'aux équivalences tautologiques mentionnées au théorème 1.3 correspondent les équivalences logiques suivantes:

$A \equiv A$;

$A \wedge A \equiv A$;

$A \vee A \equiv A$;

$A \wedge B \equiv B \wedge A$;

$A \vee B \equiv B \vee A$;

$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$;

$A \vee (B \vee C) \equiv (A \vee B) \vee C$;

$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$;
$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$;
$\neg\neg A \equiv A$;
$(A \leftrightarrow B) \equiv (B \leftrightarrow A)$;
$(A \rightarrow B) \equiv (\neg B \rightarrow \neg A)$;
$\neg (A \vee B) \equiv \neg A \wedge \neg B$;
$\neg (A \wedge B) \equiv \neg A \vee \neg B$;
$(A \leftrightarrow B) \equiv (\neg A \leftrightarrow \neg B)$;
$A \rightarrow (B \rightarrow C) \equiv B \rightarrow (A \rightarrow C)$;
$A \rightarrow B \equiv \neg A \vee B$;
$A \rightarrow B \equiv \neg (A \wedge \neg B)$;
$A \vee B \equiv \neg A \rightarrow B$;
$A \vee B \equiv \neg (\neg A \wedge \neg B)$;
$A \wedge B \equiv \neg (A \rightarrow \neg B)$;
$A \wedge B \equiv \neg (\neg A \vee \neg B)$;
$(A \leftrightarrow B) \equiv (A \rightarrow B) \wedge (B \rightarrow A)$.

Schémas déductifs. Les démonstrations de telles ou telles affirmations mathématiques s'esquissent sur la base de règles déterminées dont l'essence est traduite par des implications tautologiques de la logique des assertions. Elles donnent une image schématique de la marche de la démonstration, aussi les appelle-t-on *schémas déductifs* ou *règles des démonstrations* (voir, par exemple, plus bas règle de détachement, règle de contraposition, etc.). Donnons les règles correspondant aux 15 premières implications tautologiques du théorème 1.3:

$A,\ A \rightarrow B \models B$	règle de détachement;
$A,\ B \models A \wedge B$	règle d'inclusion de la conjonction ;
$A \wedge B \models A$, $A \wedge B \models B$	règles d'élimination de la conjonction
$A \models A \vee B$, $B \models A \vee B$	règles d'inclusion de la disjonction ;
$A \vee B,\ \neg B \models A$	règle d'élimination de la disjonction ;
$A \models \neg\neg A$	règle d'inclusion de la double négation ;
$\neg\neg A \models A$	règle d'élimination de la double négation ;

$A \to B,\ B \to A \models A \leftrightarrow B$	règle d'inclusion de l'équivalence ;
$A \leftrightarrow B \models A \to B$ $A \leftrightarrow B \models B \to A$	règles d'élimination des équivalences ;
$A \to B \models \neg B \to \neg A$	règle de contraposition ;
$\neg A \to B,\ \neg A \to \neg B \models A$	règle de démonstration *a contrario* ;
$A \to B,\ B \to C \models A \to C$	règle du syllogisme ;
$A \to C,\ B \to C \models A \vee B \to C$	démonstration par analyse des cas.

Pour noter ces règles on inscrit souvent les prémisses au-dessus de la ligne horizontale, tandis que la conclusion est placée au-dessous de cette dernière. Dans cette notation les schémas déductifs susmentionnés prennent la forme :

$$\frac{\begin{matrix} A \to B \\ A \end{matrix}}{B}$$ règle de détachement ;

$$\frac{\begin{matrix} A \\ B \end{matrix}}{A \wedge B}$$ règle d'inclusion de la conjonction ;

$$\frac{A \wedge B}{A}; \quad \frac{A \wedge B}{B}$$ règles d'élimination de la conjonction ;

$$\frac{A}{A \vee B}; \quad \frac{B}{A \vee B}$$ règles d'inclusion de la disjonction ;

$$\frac{\begin{matrix} A \vee B \\ \neg B \end{matrix}}{A}$$ règle d'élimination de la disjonction ;

$$\frac{A}{\neg\neg A}$$ règle d'inclusion de la double négation ;

$$\frac{\neg\neg A}{A}$$ règle d'élimination de la double négation ;

$$\frac{\begin{matrix} A \to B \\ B \to A \end{matrix}}{A \leftrightarrow B}$$ règle d'inclusion de l'équivalence ;

$$\frac{A \leftrightarrow B}{A \to B}; \quad \frac{A \leftrightarrow B}{B \to A}$$ règles d'élimination de l'équivalence ;

$$\frac{A \to B}{\neg B \to \neg A}$$ règle de contraposition ;

$$\frac{\begin{array}{c}\neg A \to B\\ \neg A \to \neg B\end{array}}{A}$$ règle de démonstration *a contrario* ;

$$\frac{\begin{array}{c}A \to B\\ B \to C\end{array}}{A \to C}$$ règle du syllogisme ;

$$\frac{\begin{array}{c}A \to C\\ B \to C\end{array}}{A \vee B \to C}$$ démonstration par analyse des cas.

Démonstration indirecte (démonstration *a contrario*). La collection des formules $A_1, \ldots, A_m$ de la logique des assertions est dite *contradictoire* si, pour une distribution quelconque des valeurs de vérité d'atomes qui les composent, une au moins des formules $A_1, \ldots, A_m$ acquiert la valeur F. On voit sans peine que la collection des formules $A_1, \ldots, A_m$ est contradictoire si et seulement si la formule $A_1 \wedge \ldots \wedge A_m$ est une contradiction, c'est-à-dire est une formule toujours fausse.

THÉORÈME 2.5. *Si de la collection des formules $A_1, \ldots, A_m$ il s'ensuit logiquement une contradiction, cette collection des formules est alors une contradiction.*

Démonstration. Posons que $A_1, \ldots, A_m \models F$, où F est une formule toujours fausse. Alors, selon le théorème 2.3,

$$\models A_1 \wedge \ldots \wedge A_m \to F.$$

En vertu de la table de vérité de l'implication, on en déduit que la formule $A_1 \wedge \ldots \wedge A_m$ est toujours fausse. Donc, la collection des formules $A_1, \ldots, A_m$ est une contradiction. □

Les formules toujours fausses (les contradictions) jouent un rôle essentiel dans la méthode de démonstration indirecte appelée également *méthode de démonstration a contrario.* Les démonstrations de ce type se basent sur le théorème suivant.

THÉORÈME 2.6. *Si des formules $A_1, \ldots, A_m, \neg B$ s'ensuit logiquement une contradiction, on a alors $A_1, \ldots, A_m \models B$.*

Démonstration. Posons $A_1, \ldots, A_m, \neg B \models F$, où F est une contradiction. Alors, selon le théorème 2.5, la collection des formules $A_1, \ldots, A_m, \neg B$ est contradictoire. Donc, si pour une distribution quelconque des valeurs de vérité d'atomes composant les formules $A_1, \ldots, A_m, \neg B$ toutes les formules $A_1, \ldots, A_m$ prennent la valeur V, on obtiendra pour la formule $\neg B$ la valeur F et, partant, B sera qualifié V. Donc, $A_1, \ldots, A_m \models B$. □

Ainsi, s'il faut démontrer qu'une certaine assertion B est logiquement impliquée par des prémisses données, on adjoint $\neg B$ à ces prémisses et l'on montre que de ces prémisses s'ensuit une contra-

diction (elle prend habituellement la forme $C \wedge \neg C$). Après quoi, on peut conclure que l'assertion B est la déduction logique des prémisses de départ. Pour $m = 0$ on a un cas particulier, c'est-à-dire que les prémisses manquent. Si en admettant la vérité de $\neg B$ on aboutit à la contradiction $(C \wedge \neg C)$, il devient possible d'affirmer que B est vrai. Ce raisonnement s'appuie sur la règle de la démonstration *a contrario*: $\neg B \to C, \neg B \to \neg C \models B$.

La démonstration par analyse des cas est très courante; son principe est le suivant. Supposons qu'il s'agit de démontrer la vérité de l'assertion C. On construit les assertions A et B telles que $A \vee B$, $A \to C$, $B \to C$ soient des assertions vraies (en guise de B on prend souvent non-A). Puis, sur la base du schéma déductif correspondant on peut affirmer que C est vrai.

En s'appuyant sur la règle du syllogisme on peut postuler la vérité de l'assertion $A \to B$ si l'on est en mesure de construire la chaîne des implications

$$A \to A_1, \quad A_1 \to A_2, \ldots, \quad A_{n-1} \to A_n, \quad A_n \to B,$$

dont chacune est vraie.

Exercices

1. Montrer que sont fondés les schémas déductifs suivants:

(a) $\dfrac{A \to \neg B}{B \to \neg A}$;

(b) $\dfrac{A,\ A \leftrightarrow B}{B}$;

(c) $\dfrac{A \to B}{(B \to C) \to (A \to C)}$;

(d) $\dfrac{A \leftrightarrow B,\ B \leftrightarrow C}{A \leftrightarrow C}$;

(e) $\dfrac{A \leftrightarrow B,\ C \leftrightarrow D}{A \vee C \leftrightarrow B \vee C}$;

(f) $\dfrac{A \leftrightarrow B,\ C \leftrightarrow D}{A \wedge C \leftrightarrow B \wedge D}$;

(g) $\dfrac{A \to B,\ C \to D}{A \vee C,\ B \vee D}$;

(h) $\dfrac{A \to B,\ C \to D}{A \wedge C \to B \wedge D}$;

(i) $\dfrac{A \to B,\ A \to C}{A \to B \wedge C}$;

(j) $\dfrac{A \to (B \to C)}{(A \to B) \to (A \to C)}$;

(k) $\dfrac{A \to C}{A \wedge B \to C}$;

(l) $\dfrac{A \to (B \to C)}{A \wedge B \to C}$;

(m) $\dfrac{\neg A}{A \to B}$;

(n) $\dfrac{A \to B,\ \neg B}{\neg A}$;

(o) $\dfrac{(A \wedge \neg B) \to (C \wedge \neg C)}{A \to B}$;

(p) $\dfrac{A \to (B \to C)}{B \to (A \to C)}$;

(q) $\dfrac{A \to (B \to C)}{A \to (\neg C \to \neg B)}$.

2. Démontrer que pour toute formule de la logique des assertions il existe une formule d'équivalence logique construite seulement à l'aide de l'un des

couples suivants de copules:

(a) $\neg, \rightarrow$; (b) $\neg, \vee$; (c) $\neg, \wedge$.

3. Démontrer que

(a) $\neg A \vee B,\ C \rightarrow \neg B \models A \rightarrow \neg C$;
(b) $A \vee B,\ A \rightarrow C,\ B \rightarrow D \models C \vee D$;
(c) $A \rightarrow (B \rightarrow C),\ \neg D \vee A,\ B \models D \rightarrow C$;
(d) $A \vee B \rightarrow C \wedge D,\ D \vee E \rightarrow F \models A \rightarrow F$.

§ 3. Prédicats

Les moyens offerts par la logique des assertions s'avèrent insuffisants pour analyser de nombreux raisonnements mathématiques. Par exemple, la logique des assertions ne permet pas d'établir la validité du raisonnement suivant: « Tout nombre entier est un nombre rationnel; 25 est un nombre entier, donc 25 est un nombre rationnel ». Car en logique des assertions les assertions simples à partir desquelles sont construites les assertions complexes sont stipulées indivisibles. Elles ne sont pas soumises à l'analyse de la structure au sens des relations entre les objets et leurs propriétés. Aussi, s'avère-t-il nécessaire de construire un système logique dont les règles permettent d'étudier la structure d'assertions considérées en logique des assertions comme élémentaires. Ce système est la logique des prédicats dont la logique des assertions constitue une des parties.

Variables libres. On utilise largement en mathématiques des notations littérales. Certaines lettres mises en relief dans le texte désignent des objets quelconques d'une certaine classe. Chacune de ces lettres conserve généralement son individualité, c'est-à-dire désigne toujours le même objet tout au long d'une certaine partie du texte. Des lettres différentes peuvent être affectées soit à un même objet, soit à des objets différents. Les lettres ainsi utilisées sont appelées *variables libres*.

On appelle *valeurs spécifiées* de la variable libre les objets de la classe déterminée pour la notation desquels on a utilisé cette variable. C'est ainsi que les valeurs spécifiées de la variable libre peuvent être des assertions. Une telle variable libre est dénommée *propositionnelle*.

Les valeurs spécifiées de la variable libre peuvent être des nombres naturels ou entiers. Une telle variable libre s'appelle alors respectivement *naturelle* ou *entière*.

Si les valeurs spécifiées de la variable libre sont des nombres réels ou complexes, alors cette variable est appelée respectivement *réelle* ou *complexe*.

Prédicats. Soit une proposition

(1) $x + y = 3$

contenant des variables naturelles x et y. Cette proposition n'est pas une assertion car on ne peut répondre à la question: Est-elle vraie ou bien est-elle fausse? On l'appelle *prédicat* ou *condition* (sur x et y). Donnons d'autres exemples de propositions avec variables:

(2) x est un nombre premier;
(3) x est un nombre pair;
(4) x est plus petit que y;
(5) x est le diviseur commun de y, z.

Posons que les valeurs spécifiées des variables x, y et z sont des nombres naturels. Si dans les propositions (1)-(5) on remplace les variables par leurs valeurs spécifiées, on obtiendra des assertions qui pourront être aussi bien vraies que fausses. Par exemple,

$0 + 1 = 3$;
2 est un nombre premier;
3 est un nombre pair;
5 est inférieur à 7;
3 est le diviseur commun de 6 et 12.

DÉFINITION. Les propositions avec variables aboutissant à des assertions après substitution aux variables libres de leurs valeurs spécifiées sont appelées *prédicats.*

Les propositions (1)-(5) peuvent être prises pour des exemples de prédicats.

Suivant le nombre de variables libres composant les prédicats on distingue les prédicats *à une place* (monadiques), *à deux places* (diadiques), *à trois places* (triadiques), etc. Les prédicats (2) et (3) sont à une place, les prédicats (1) et (4) à deux places, le prédicat (5) est à trois places. Les assertions seront considérées comme des prédicats à aucune place.

En remplaçant dans le prédicat à une place (2) la variable par des nombres naturels on aboutit aux assertions:

0 est un nombre premier;
1 est un nombre premier;
2 est un nombre premier;
3 est un nombre premier, etc.

Certaines de ces assertions sont vraies. C'est ainsi que le prédicat donné à une place détermine parmi les nombres naturels ceux qui, une fois substitués à la variable, fournissent une assertion vraie; il

peut donc être assimilé à une condition imposée à la valeur de la variable libre composant le prédicat. Dans l'exemple considéré les nombres satisfaisant à cette condition sont les nombres premiers.

Un prédicat à une place peut être assimilé à une condition imposée à des objets de la classe donnée; un prédicat à deux places à une condition imposée à un couple d'objets de même classe, etc.

Les prédicats peuvent être posés de façons différentes. En algèbre on étudie souvent des prédicats posés au moyen d'équations, d'inégalités, ainsi qu'au moyen de systèmes d'équations ou d'inégalités. C'est ainsi, par exemple, que l'inégalité $x + x^{-1} > 0$ définit un prédicat à une place, l'équation $x^2 + y = 0$ un prédicat à deux places, tandis que le système d'équations $x + y = 0, x - y + z = 0$ définit un prédicat à trois places (x, y, z étant des variables rationnelles).

On notera les prédicats par des capitales latines (avec indice inférieur si nécessaire) avec indication entre parenthèses de toutes les variables libres composant le prédicat. Par exemple, $A(x, y)$ est la notation d'un prédicat à deux places, $R(x, y, z)$ celle d'un prédicat à trois places et $Q(x_1, \ldots, x_n)$ celle d'un prédicat à n places (n-adique).

Par la suite, on parlera de la valeur de vérité d'un prédicat quelconque sur un certain jeu de variables libres qui le composent en entendant par là la valeur de vérité de l'assertion obtenue par substitution aux variables libres des valeurs correspondantes du jeu considéré.

L'assertion obtenue en portant dans le prédicat $R(x_1, \ldots, x_n)$ le jeu de valeurs spécifiées $(a_1, \ldots, a_n)$ au lieu de ses variables sera notée $R(a_1, \ldots, a_n)$. Si cette assertion est vraie (fausse) on dit que ce jeu de valeurs $(a_1, \ldots, a_n)$ satisfait (ou ne satisfait pas) au prédicat $R(x_1, \ldots, x_n)$.

Notons qu'il faut distinguer les prédicats exprimant une même condition, mais composés de variables aux valeurs spécifiées différentes. Par exemple, le prédicat défini par l'équation $2x - 3 = 0$, où x est une variable entière, doit être distingué du prédicat défini par la même équation avec x considéré comme une variable rationnelle. Le premier prédicat n'est qualifié vrai pour aucune des valeurs spécifiées de x, tandis que le second est vrai pour la valeur spécifiée de $x = 3/2$. En définissant un prédicat on doit donc indiquer le domaine des valeurs spécifiées des variables de ce prédicat.

Opérations sur les prédicats. Les prédicats, comme les assertions, sont qualifiés V et F et peuvent ainsi être soumis à des opérations logiques analogues à celles de la logique des assertions.

Commençons par un cas particulier simple, celui des prédicats à une place dont les domaines des valeurs spécifiées des variables coïncident. A partir de deux prédicats $P(x)$ et $Q(y)$ formons un nouveau prédicat $P(x) \wedge Q(y)$. C'est un prédicat à deux variables libres x

et y et sa valeur de vérité pour tout jeu (a, b) de valeurs spécifiées des variables se définit comme la valeur de vérité de l'assertion $P(a) \wedge P(b)$. De façon analogue se définissent les prédicats

$$P(x) \vee Q(y), \quad \neg P(x), \quad P(x) \rightarrow Q(y), \quad P(x) \leftrightarrow Q(y).$$

Il faut distinguer les prédicats: à deux places $P(x) \wedge Q(y)$ de celui à une place $P(x) \wedge Q(x)$; dans le premier on spécifie les variables libres x et y indépendamment l'une de l'autre, et dans le second, la variable libre x uniquement.

On définit de façon analogue pour les prédicats à plusieurs places (polyadiques) les opérations de conjonction, de disjonction, de négation, d'implication et d'équivalence. Voyons, par exemple, le cas de prédicats à deux places. Soient $P(x, y)$, $Q(y, z)$ deux prédicats dont les domaines des variables spécifiées coïncident. $P(x, y) \wedge \wedge Q(y, z)$ est alors un prédicat à trois places en x, y, z dont la valeur de vérité pour tout jeu des variables libres spécifiées (a, b, c) est définie comme la valeur de l'assertion $P(a, b) \wedge Q(b, c)$. Notons qu'en analysant les opérations sur les prédicats il faut distinguer les variables désignées par des lettres différentes de celles désignées par des lettres identiques.

Voyons encore quelques exemples:

1) $A(x) \vee B(x, y)$ prédicat par rapport aux variables libres x et y;

2) $\neg A(y) \wedge D(z, x)$ prédicat par rapport aux variables libres x, y, z;

3) $E(x, y, z) \rightarrow F(z)$ prédicat par rapport aux variables libres x, y, z.

Le prédicat $A(x) \vee B(x, y)$ acquiert la valeur V pour le jeu des valeurs (a, b) si l'une au moins des assertions $A(a)$ et $B(a, b)$ est vraie et, prend la valeur F si ces deux assertions sont fausses. De façon analogue, on peut établir les valeurs de vérité des autres prédicats pour un jeu donné de variables libres.

Déduction logique. Prédicats équipotents.

DÉFINITION. Le prédicat $A(x_1, \ldots, x_n)$ est dit *toujours vrai* si pour tout jeu de valeurs spécifiées des variables libres qui le composent sa valeur de vérité est V.

On peut prendre pour exemple de prédicat toujours vrai le prédicat à trois places défini par l'inégalité $(x + y)^2 + z^2 \geqslant 0$, où x, y, z sont des variables rationnelles.

Soient $A(x_1, \ldots, x_m)$ et $B(y_1, \ldots, y_n)$ les prédicats possédant des domaines identiques de variables libres spécifiées.

DÉFINITION. Le prédicat $B(y_1, \ldots, y_n)$ est dit *déduction logique du prédicat* $A(x_1, \ldots, x_m)$ si le prédicat $A(x_1, \ldots, x_m) \rightarrow \rightarrow B(y_1, \ldots, y_n)$ est identiquement vrai.

La notation $A(x_1, \ldots, x_m) \models B(y_1, \ldots, y_n)$ signifie que le prédicat $B(y_1, \ldots, y_n)$ est la déduction logique du prédicat $A(x_1, \ldots, x_m)$.

Par exemple, si x est une variable entière, $R(x)$ la notation du prédicat « x est un nombre pair », $P(x)$ la notation du prédicat « x est multiple de 4 », alors $R(x)$ s'ensuit logiquement de $P(x)$, autrement dit, $P(x) \models R(x)$. Dans ce cas le prédicat $R(x)$ n'entraîne pas logiquement $P(x)$.

Prenons deux prédicats à n places $A(x_1, \ldots, x_n)$ et $B(x_1, \ldots, x_n)$ concernant les mêmes variables libres. Le prédicat $B(x_1, \ldots, x_n)$ sera la déduction logique du prédicat $A(x_1, \ldots, x_n)$ si et seulement si tout jeu de valeurs des variables $x_1, \ldots, x_n$, satisfaisant au prédicat $A(x_1, \ldots, x_n)$, satisfait également au prédicat $B(x_1, \ldots, x_n)$.

On laisse au lecteur le soin d'esquisser la démonstration de cette affirmation.

Définition. Le prédicat $B(z_1, \ldots, z_n)$ est dit *déduction logique* des prédicats $A_1(x_1, \ldots, x_m), \ldots, A_k(y_1, \ldots, y_l)$ si le prédicat

$$A(x_1, \ldots, x_m) \wedge \ldots \wedge A_k(y_1, \ldots, y_l) \rightarrow B(z_1, \ldots, z_n)$$

est identiquement vrai. (On suppose dans ce cas que toutes les variables libres des prédicats considérés possèdent les mêmes valeurs spécifiées.)

Exemple. Soit $P(x)$ le prédicat « x est un nombre pair », $Q(x)$ le prédicat « x est multiple de 3 », $R(x)$ le prédicat « x est multiple de 6 ». Alors, $P(x), Q(x) \models R(x)$.

Définition. Les prédicats $A(x_1, \ldots, x_m)$ et $B(y_1, \ldots, y_n)$ sont dits *équipotents* (*logiquement équivalents*) si le prédicat $A(x_1, \ldots, x_m) \leftrightarrow B(y_1, \ldots, y_n)$ est identiquement vrai. La notation $A(x_1, \ldots, x_m) \equiv B(y_1, \ldots, y_n)$ signifie que les prédicats $A(x_1, \ldots, x_m)$ et $B(y_1, \ldots, y_n)$ sont équipotents.

On voit sans peine que les prédicats $A(x_1, \ldots, x_m)$ et $B(y_1, \ldots, y_n)$ sont équipotents si et seulement si

$$A(x_1, \ldots, x_m) \models B(y_1, \ldots, y_n) \quad \text{et} \quad B(y_1, \ldots, y_n) \models A(x_1, \ldots, x_m).$$

Il est facile de démontrer que les prédicats $A(x_1, \ldots, x_m)$ et $B(x_1, \ldots, x_n)$ sont équipotents si et seulement si leurs valeurs de vérité coïncident pour tout jeu de valeurs spécifiées des variables $x_1, \ldots, x_n$. On peut donner en guise d'exemple de prédicats équipotents les prédicats définis par les équations $x^3 - y^3 = 0$ et $2(x - y)(x^2 + xy + y^2) = 0$, où x, y sont des variables rationnelles.

Définition. Le prédicat $A(x_1, \ldots, x_n)$ est dit *identiquement faux* si sa valeur de vérité est qualifiée F pour tout jeu de valeurs spécifiées des variables libres qui y figurent.

Par exemple, est identiquement faux le prédicat $x + 1 = x$, où x est une variable entière.

DÉFINITION. Le prédicat $A(x_1, \ldots, x_n)$ est dit *réalisable* s'il y a au moins un jeu de valeurs spécifiées des variables libres y figurant pour lequel sa valeur de vérité est V.

Par exemple, sont réalisables les prédicats tels que « x est un nombre premier », « x est divisible par y », « $x^2 - 5x + 6 = 0$ », où x est une variable entière.

Des définitions susmentionnées il s'ensuit qu'un prédicat identiquement vrai se déduit logiquement de tout prédicat, tandis que d'un prédicat identiquement faux s'ensuit logiquement tout prédicat.

Tout prédicat est soit identiquement vrai, soit réalisable, soit identiquement faux.

Exercices

1. Donner des exemples de prédicats $P(x, y, z)$ et $R(x, y, z)$, où x, y, z sont des variables naturelles, dont l'un est une déduction logique de l'autre.
2. Donner des exemples de prédicats à une, deux et trois places qui soient identiquement faux, identiquement vrais et réalisables (mais non pas identiquement vrais).
3. Construire les prédicats $A(x)$ et $B(x)$, où x est une variable entière, de manière que
(a) les prédicats $A(x)$ et $B(x)$ soient non identiquement vrais, tandis que $A(x) \vee B(x)$ le soit;
(b) $A(x)$ et $B(x)$ soient des prédicats réalisables, et $A(x) \wedge B(x)$ un prédicat non réalisable.

§ 4. Quantificateurs

Examinons de nouvelles opérations qui appliquées aux prédicats ou bien aux assertions fournissent, une fois réalisées, des prédicats ou des assertions. Ces opérations constituent des expressions d'universalité ou d'existence.

Quantificateur universel. Soit $A(x)$ le prédicat à une variable libre x. Par l'expression $\forall x A(x)$ on désignera l'assertion qui sera vraie si $A(x)$ acquiert la valeur V pour toutes les valeurs spécifiées de la variable x, c'est-à-dire si le prédicat $A(x)$ est identiquement vrai, et la valeur F dans le cas contraire. L'assertion $\forall x A(x)$ est ainsi indépendante de x. Le symbole $\forall x$ placé à gauche du prédicat $A(x)$ est appelé *quantificateur universel* suivant la variable x. Si, par contre, A est une assertion, $\forall x A$ est alors une assertion vraie si et seulement si A est vrai.

Passons maintenant à un prédicat à plusieurs variables libres, par exemple le prédicat $A(x, y, z)$ de trois variables. Ce prédicat, après la substitution arbitraire de toutes les variables libres, sauf x, par leurs valeurs b et c, constitue un prédicat concernant seulement

la variable libre x, et l'expression

$$\forall x A\ (x,\ b,\ c)$$

est une assertion. Le prédicat $\forall x A\ (x, y, z)$ se transforme en une assertion après la spécification de toutes les variables libres qui le composent, sauf x, et, partant, ne dépend pas de x. $\forall x A\ (x, y, z)$ est ainsi fonction de toutes les variables libres composant $A\ (x, y, z)$, sauf x, c'est donc un prédicat à deux places concernant y et z. Ce prédicat pour le jeu donné des valeurs des variables libres b, c est qualifié V si et seulement si le prédicat $A\ (x, b, c)$ ne dépendant que d'une seule variable libre x est identiquement vrai. Le symbole $\forall x$ se lit « quel que soit x » ou « pour tout x », tandis que la notation $\forall x A\ (x, y, z)$ se lit « quel que soit x on a $A\ (x, y, z)$ » ou, de façon plus concise, « pour tout x $A\ (x, y, z)$ ».

La variable x dont le prédicat $\forall x A\ (x, y, z)$ ne dépend pas est appelée *variable liée* (pour la différencier des variables y, z qui sont des variables libres).

Quantificateur existentiel. On utilise pour le quantificateur existentiel le symbole $\exists x$ placé à gauche du prédicat ou de l'assertion. Soit $A\ (x)$ un prédicat à variable libre x. Par l'expression $\exists x A\ (x)$ on comprendra l'assertion vraie si $A\ (x)$ est qualifié V au moins pour une des valeurs spécifiées de la variable x, (le prédicat $A\ (x)$ est réalisable), et fausse, dans le cas contraire. Si, par contre, A est une assertion, $\exists x A$ est aussi une assertion qui est vraie si et seulement si A est vrai.

Supposons maintenant que $A\ (x, y, z)$ est un prédicat à trois places. Si dans ce prédicat à toutes les variables libres, sauf x, on substitue leurs valeurs, par exemple, b, c, on obtiendra alors le prédicat $A\ (x, b, c)$ qui ne dépend que d'une variable libre x, et l'expression

$$\exists x A\ (x,\ b,\ c)$$

sera une assertion. Donc l'expression $\exists x A\ (x, y, z)$ est un prédicat qui se transforme en une assertion après spécification de toutes les variables libres, sauf x, et, par suite, ne dépend pas de x. Ainsi, l'expression $\exists x A\ (x, y, z)$ est un prédicat qui n'est fonction que de y et z, vu que l'application d'un quantificateur au prédicat à trois places le fait passer à un prédicat à deux places. La variable x dont le prédicat $\exists x A\ (x, y, z)$ ne dépend pas est appelée *variable liée*.

Le prédicat $\exists x A\ (x, y, z)$ prend la valeur V avec le jeu donné des valeurs spécifiées b, c si et seulement si le prédicat à une place $A\ (x, b, c)$ est réalisable.

Le symbole $\exists x$ est appelé *quantificateur existentiel* suivant la variable x et se lit : « il existe un x ». L'expression $\exists x A\ (x, y, z)$

se lit: « $A(x, y, z)$ existe au moins pour un x » ou bien: « il existe un x tel que $A(x, y, z)$ ».

On applique les quantificateurs de façon absolument analogue à des prédicats à un nombre de variables plus grand. L'association d'un quantificateur à un prédicat à n places (pour $n > 0$) transforme ce dernier en un prédicat à $(n - 1)$ places.

A un même prédicat il est possible d'associer à plusieurs reprises des quantificateurs. Par exemple, après avoir associé au prédicat $A(x, y)$ le quantificateur existentiel suivant x, on obtient le prédicat à une place $\exists x A(x, y)$ auquel on peut associer de nouveau le quantificateur existentiel ou bien le quantificateur universel suivant la variable y. Finalement on obtient l'assertion

$$\exists y (\exists x A(x, y)) \quad \text{ou bien} \quad \forall y (\exists x A(x, y)).$$

Habituellement on supprime les parenthèses et on obtient les expressions

$$\exists y \, \exists x A(x, y) \quad \text{ou bien} \quad \forall y \, \exists x A(x, y).$$

Notons que les quantificateurs identiques peuvent être permutés en obtenant des assertions équivalentes, autrement dit, des équivalences vraies:

$$\forall x \forall y (x, y) \leftrightarrow \forall y \forall x A(x, y);$$

$$\exists x \exists y A(x, y) \leftrightarrow \exists y \exists x A(x, y).$$

En effet, les assertions $\forall x \forall y A(x, y)$ et $\forall y \forall x A(x, y)$ sont toutes les deux vraies si et seulement si le prédicat $A(x, y)$ est identiquement vrai. Les assertions $\exists x \exists y (x, y)$ et $\exists y \exists x A(x, y)$ sont toutes les deux vraies si et seulement si $A(x, y)$ est un prédicat réalisable. Toutefois, si l'on associe au prédicat successivement des quantificateurs différents, l'ordre de leur succession est alors essentiel. Par exemple, les assertions $\forall y \exists x A(x, y)$ et $\exists x \exists y A(x, y)$ ne sont pas à proprement parler équivalentes, c'est-à-dire qu'elles peuvent avoir des valeurs de vérité différentes.

L'association à un prédicat d'un ou de plusieurs quantificateurs (universel, existentiel) est appelée *quantification*.

Voyons sur un exemple comment on applique les quantificateurs. Soit $x + y > 0$ un prédicat à deux places, où x et y sont des variables entières. Ce prédicat exprime la positivité d'une somme de deux nombres entiers et constitue une assertion chaque fois quand les variables x et y sont spécifiées. Si l'on associe à ce prédicat un quantificateur existentiel suivant y on le transforme en un prédicat à une place

$$\exists y (x + y > 0).$$

Quand on spécifie la variable x de ce prédicat, ce dernier devient une assertion. Le prédicat $\exists y (x + y > 0)$ est vrai quand les valeurs

de la variable x fournissent un entier y formant sommé avec x un nombre positif. On se convainc sans peine que ce prédicat est identiquement vrai, et si on associe à ce dernier un quantificateur universel en x, on obtient alors l'assertion

$$\forall x \exists y \, (x + y > 0),$$

postulant que pour tout nombre entier x il existe un certain nombre entier y rendant leur somme positive. Cette assertion est à distinguer de l'assertion

$$\exists y \forall x \, (x + y > 0),$$

affirmant qu'il existe un nombre entier dont la somme avec tout nombre entier est positive. Cette dernière assertion est fausse.

Notation des assertions dans le language de la logique des prédicats. Examinons quatre types principaux d'assertions qu'on rencontre fréquemment en mathématiques. Dans la notation symbolique de ces assertions (le langage de la logique des prédicats) on utilise les quantificateurs.

Soit $A\ (x)$ la notation du prédicat « x est un nombre impair » et $B\ (x)$ la notation du prédicat « x est un nombre premier », où x est une variable entière.

1. L'assertion « Tout nombre impair est un nombre premier » peut être réénoncée de la façon suivante : « Pour tout x, si x est impair, x est un nombre premier ». Il devient alors clair que dans le langage des prédicats cette assertion se notera ainsi :

$$\forall x \, (A\ (x) \rightarrow B\ (x)).$$

2. L'assertion « Aucun nombre impair ne constitue un nombre premier » ou « Pour tout x, si x est impair, x n'est pas premier » se notera symboliquement ainsi :

$$\forall x \, (A\ (x) \rightarrow \neg B\ (x)).$$

Remarquons que dans nos raisonnements la valeur de vérité de l'assertion ne joue aucun rôle.

3. Le type suivant d'assertion est de la forme : « Certains nombres impairs sont premiers ». Elle veut dire qu'il existe un x qui est simultanément impair et premier. Aussi l'assertion du troisième type se notera-t-elle dans le langage des prédicats sous la forme

$$\exists x \, (A\ (x) \wedge B\ (x)).$$

Cette dernière notation n'est pas équivalente à la notation

$$\exists x \, (A\ (x) \rightarrow B\ (x)),$$

dont le sens est différent à celui de l'assertion de départ.

4. Le quatrième type d'assertions est de la forme: « Certains nombres impairs ne sont pas premiers ». Cette assertion se note ainsi:

$$\exists x\ (A\ (x) \wedge \neg\ B\ (x)).$$

Les exemples examinés montrent que chaque assertion appartenant à l'un des quatre principaux types se prête à une notation symbolique.

Dans la suite pour énoncer l'assertion « Il existe un x positif tel que $A\ (x)$ », au lieu de la notation symbolique

$$\exists x\ (x > 0 \wedge A\ (x)),$$

on utilisera une notation plus concise $(\exists x > 0)\ A\ (x)$. De façon analogue pour l'assertion « Pour tout x positif on a $A\ (x)$ » au lieu de

$$\forall x\ (x > 0 \rightarrow A\ (x))$$

on se servira de la notation $(\forall x > 0)\ A\ (x)$.

Exercices

1. Ecrire dans le langage des prédicats les assertions suivantes:
(a) Certains nombres réels sont des nombres rationnels.
(b) Aucun nombre premier n'est un carré exact.
(c) Certains nombres pairs ne se divisent pas par 8.
(d) Tout multiple de 6 se divise par 3.

2. $P\ (x)$ désigne « x est un nombre premier », $Q\ (x)$ « x est un nombre pair », $R\ (x)$ « x est un nombre entier », $D\ (x,\ y)$ « x divise y ». Formuler en se servant des mots les assertions suivantes notées dans le langage des prédicats. Distinguer celles qui sont vraies de celles qui sont fausses:

(a) $\forall x P\ (x) \rightarrow \neg Q\ (x)$;

(b) $\forall x\ (\neg P\ (x) \rightarrow \forall y\ (P\ (y) \rightarrow \neg D\ (x,\ y)))$;

(c) $\forall x\ (Q\ (x) \rightarrow \forall y\ (D\ (x,\ y) \rightarrow Q\ (y)))$;

(d) $\forall x \exists y\ (R\ (x) \wedge R\ (y) \rightarrow D\ (x,\ y))$;

(e) $\forall y \forall x\ (R\ (x) \wedge R\ (y) \rightarrow D\ (x,\ y))$;

(f) $\exists x \forall y\ (R\ (x) \wedge R\ (y) \rightarrow D\ (x,\ y))$.

3. En se servant des symboles logiques écrire les assertions suivantes:
(a) Les nombres 5 et 12 n'ont pas de communs diviseurs différents de $+1$ et -1.
(b) Le nombre naturel divisible par 6 est également divisible par 2 et par 3.
(c) Pour tout nombre entier x il existe un nombre entier y vérifiant soit $x = 2y$, soit $x = 2y + 1$.
(d) Tout nombre naturel a un nombre naturel supérieur à lui.
(e) Il existe un nombre naturel minimal.
(f) Le système d'équations $x + y = 0$, $x + y = 1$ n'admet pas de solution (système incompatible).
(g) Il n'existe pas de nombre rationnel x tel que $x^2 - 2 = 0$.
(h) Pour tous nombres entiers x et z il existe un nombre entier y tel que $x + y = z$.

(i) Pour tous deux nombres rationnels x et y il existe un nombre rationnel z tel que $x < z$ et $z < y$.

4. Chercher si pour tous prédicats $P(x, y)$, $Q(x)$, $R(x)$ on a les équipotences suivantes. Si non, donner des exemples de prédicats qui le confirment:

(a) $\forall x \exists y P(x, y) \equiv \exists y \forall x P(x, y)$;

(b) $\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y)$;

(c) $\forall x (R(x) \vee Q(x)) \equiv \forall x R(x) \vee \forall x Q(x)$;

(d) $\exists x (R(x) \wedge Q(x)) \equiv \exists x R(x) \wedge \exists x Q(x)$;

(e) $\forall x \forall y (R(x) \vee Q(y)) \equiv \forall x R(x) \vee \forall x Q(x)$;

(f) $\forall x Q(x) \to \exists x R(x) \equiv \exists x (Q(x) \to R(x))$;

(g) $\exists x R(x) \vee \forall x Q(x) \equiv \exists x (R(x) \to Q(x))$;

(h) $\forall x (R(x) \to Q(x)) \equiv \forall x R(x) \to \forall x Q(x)$.

§ 5. Formules des prédicats. Lois logiques

Formules élémentaires. Supposons qu'on dispose d'une liste de variables

$$x, y, z, u, w, \ldots, x_1, y_1, z_1, u_1, w_1, \ldots,$$

appelées souvent *objets variables*, car on leur substitue des noms d'objets déterminés

$$a, b, c, a_1, b_1, c_1, \ldots$$

En outre on admet que pour chaque n naturel on possède un certain ensemble d'expressions

$$P(x_1, x_2, \ldots, x_n), \quad Q(x, y, \ldots, t), \quad R(y_1, \ldots, y_n), \ldots,$$

appelées *symboles prédicatifs* n-aires (à n places). Par exemple, $P(x)$, $Q(y)$ sont des symboles prédicatifs singulaires (à une place), $P(x, y)$, $Q(x_1, x_2)$ binaires (à deux places), $P(x, y, z)$, $R(x_1, x_2, x_3)$ ternaires (à trois places), $A, B, \ldots, P, Q$ zéronaires (à aucune place). En partant de cette collection de symboles prédicatifs on forme des expressions qu'on appellera formules élémentaires ou prédicats atomiques de la logique (atomes de la logique des prédicats).

Définition. On appelle *formule élémentaire* l'expression obtenue par substitution dans le symbole prédicatif aux variables $(x, y, \ldots)$ qui le composent de certains objets variables non obligatoirement distincts.

Par exemple, en partant du symbole prédicatif singulaire $P(x)$, on aboutit aux formules élémentaires (atomes) $P(x)$, $P(y)$, $P(u)$, etc.; en partant du symbole prédicatif binaire $Q(x, y)$, on obtient les formules élémentaires $Q(x, y)$, $Q(y, z)$, $Q(u, v)$, $Q(x, x)$, etc. En partant du symbole prédicatif $R(x, y, z)$, on a les formules élémentaires $R(x, y, z)$, $R(y, z, x)$, $R(u, v, w)$, $R(x, x, x)$,

$R(x, y, x)$, etc. Les symboles prédicatifs initiaux à aucune place sont aussi inclus dans la collection des formules élémentaires. Les formules élémentaires constituent une collection plus vaste que la collection de départ des symboles prédicatifs, vu que les objets variables entrant dans les formules élémentaires ne sont pas obligatoirement distincts.

Formules prédicatives. Les *formules prédicatives* (formules de la logique des prédicats) s'introduisent de la façon suivante:

(a) toute formule élémentaire est une formule prédicative;

(b) si **A** et **B** sont des formules prédicatives, $(\neg \mathbf{A})$, $(\mathbf{A} \wedge \mathbf{B})$, $(\mathbf{A} \vee \mathbf{B})$, $(\mathbf{A} \rightarrow \mathbf{B})$ et $(\mathbf{A} \leftrightarrow \mathbf{B})$ sont aussi des formules prédicatives. Si **A** est une formule prédicative et x un objet variable, $(\forall x\mathbf{A})$ et $(\exists x\mathbf{A})$ sont aussi des formules prédicatives;

(c) une expression n'est une formule prédicative que si elle est une formule élémentaire ou si elle est construite avec des formules élémentaires par application successive des règles (a), (b).

Les formules prédicatives qui ne sont pas élémentaires sont dites *formules prédicatives composées.*

Pour la notation des formules de la logique des prédicats on se servira de capitales latines en caractère gras: **A**, **B**, **C**, . . ., **R**, **P**, **Q**, etc.

Dans les formules $(\forall x\mathbf{A})$ et $(\exists x\mathbf{A})$ la formule **A** est appelée *domaine d'action des quantificateurs* $\forall x$ et $\exists x$ respectivement.

On convient habituellement de supprimer les parenthèses. De plus, on pose que les quantificateurs ont une force liante supérieure à celle des autres opérations. Aussi la formule $(\forall xP(x)) \rightarrow R(x, y)$ peut-elle s'écrire: $\forall xP(x) \rightarrow R(x, y)$.

DÉFINITION. La formule prédicative est dite *universelle* si après remplacement des formules élémentaires la composant par des prédicats quelconques, on obtient un prédicat toujours vrai.

DÉFINITION. Les formules prédicatives sont dites *équipotentes* si après substitution aux formules élémentaires qui les composent des formules prédicatives quelconques, on aboutit à des prédicats équipotents. L'équipotence des formules **A** et **B** se notera ainsi: $\mathbf{A} \equiv \mathbf{B}$.

On démontre sans peine que la formule prédicative $\mathbf{A} \leftrightarrow \mathbf{B}$ est universelle si et seulement si **A** et **B** sont des formules prédicatives équipotentes.

Une série d'équipotences de la logique des prédicats peut être obtenue des équipotences de la logique des assertions. Par exemple, aux équipotences de la logique des assertions

$$A \wedge B \equiv B \wedge A;$$
$$\neg\neg A \equiv A;$$
$$\neg(A \vee B) \equiv \neg A \wedge \neg B;$$
$$\neg(A \wedge B) \equiv \neg A \vee \neg B$$

correspondent des équipotences de la logique des prédicats

$\mathbf{A} \wedge \mathbf{B} \equiv \mathbf{B} \wedge \mathbf{A}$;

$\neg\neg \mathbf{A} \equiv \mathbf{A}$;

$\neg (\mathbf{A} \vee \mathbf{B}) \equiv \neg \mathbf{A} \wedge \neg \mathbf{B}$;

$\neg (\mathbf{A} \wedge \mathbf{B}) \equiv \neg \mathbf{A} \vee \neg \mathbf{B}$.

De façon analogue les formules identiquement vraies de la logique des assertions constituent la source d'où sont puisées les formules universelles de la logique des prédicats. Par exemple, à la tautologie $A \vee \neg A$ correspond la formule universelle de la logique des prédicats $\mathbf{A} \vee \neg \mathbf{A}$. En effet, en portant des prédicats quelconques dans toute formule **A** concrète au lieu des symboles prédicatifs qui la composent, on obtient un certain prédicat $P(x_1, \ldots, x_n)$. La formule $\mathbf{A} \vee \neg \mathbf{A}$ se transforme dans ce cas en prédicat $P(x_1, \ldots, x_n) \vee \vee \neg P(x_1, \ldots, x_n)$ qui acquiert la valeur V pour toutes valeurs spécifiées des variables (en vertu de la loi du tiers exclu de la logique des assertions).

En raisonnant de même, on est en mesure de valider les autres formules universelles et équipotences de la logique des prédicats transférées de la logique des assertions.

Outre les formules universelles et les équipotences de la logique des prédicats obtenues de la sorte, il existe des formules universelles et des équipotences spécifiques en rapport avec le recourt aux quantificateurs. On en examinera quelques unes.

Lois de la logique des prédicats. Etudions une série d'équipotences jouant un grand rôle en logique des prédicats. On n'esquissera pas de démonstration rigoureuse. L'équipotence

(1) $\neg (\forall x A(x)) \equiv \exists x (\neg A(x))$

correspond à l'interprétation habituelle des quantificateurs. Les assertions « Il est faux que tout objet x satisfait à la condition $A(x)$ » et « Il existe un objet x qui ne satisfait pas à la condition $A(x)$ » ont la même signification exprimant l'équipotence (1).

L'équipotence

(2) $\neg (\exists x A(x)) \equiv \forall x (\neg A(x))$

correspond à l'identification habituelle des assertions « Il est faux qu'il existe un objet x satisfaisant à la condition $A(x)$ » et « Aucun objet x ne satisfait à la condition $A(x)$ ».

En appliquant la négation aux deux membres de (1) et (2) et, compte tenu de la loi de la double négation, on aboutit encore à deux équipotences

(3) $\forall x A(x) \equiv \neg (\exists x \neg A(x))$;

(4) $\exists x A(x) \equiv \neg (\forall x \neg A(x))$;

ces dernières montrent que le quantificateur existentiel peut s'exprimer au moyen du quantificateur universel et réciproquement.

Les deux équipotences suivantes traduisent les propriétés de distributivité du quantificateur universel relativement à la conjonction et du quantificateur existentiel relativement à la disjonction:

(5) $\exists x A(x) \vee \exists x B(x) \equiv \exists x (A(x) \vee B(x))$;

(6) $\forall x A(x) \wedge \forall x B(x) \equiv \forall x (A(x) \wedge B(x))$.

A la vérité de ces équipotences sont reliés les importants raisonnements suivants. Le premier membre de (5) acquiert la valeur V si et seulement si ou bien $A(x)$, ou bien $B(x)$ sont qualifiés V au moins pour une valeur spécifiée de x, c'est-à-dire quand au moins un des prédicats $A(x)$ et $B(x)$ est valide. Or, c'est justement dans ce cas et rien que dans ce cas que sera valide le prédicat $A(x) \vee B(x)$, c'est-à-dire sera vraie l'assertion $\exists x (A(x) \vee B(x))$. Des raisonnements analogues peuvent être conduits pour l'équipotence (6).

Le quantificateur existentiel n'est pas distributif relativement à la conjonction, c'est-à-dire que les formules $\exists x (A(x) \wedge B(x))$ et $\exists x A(x) \wedge \exists x B(x)$ ne sont pas équipotentes. Il n'est pas difficile de trouver un exemple de deux prédicats réalisables dont la conjonction soit non réalisable. Pour de tels prédicats la première formule est qualifiée F, et la seconde, V. Les formules $\forall x (A(x) \vee B(x))$ et $\forall x A(x) \vee \forall x B(x)$ sont de même non équipotentes, autrement dit, le quantificateur universel n'est pas distributif relativement à la disjonction.

A chaque équipotence de la logique des prédicats correspond une formule universelle. Par exemple, seront universelles les formules suivantes (on les appelle souvent *lois logiques*):

(1) $\neg (\forall x \mathbf{A}(x)) \leftrightarrow \exists x (\neg \mathbf{A}(x))$;

(2) $\neg (\exists x \mathbf{A}(x)) \leftrightarrow \forall x (\neg \mathbf{A}(x))$;

(3) $\forall x \mathbf{A}(x) \leftrightarrow \neg (\exists x \neg \mathbf{A}(x))$;

(4) $\exists x \mathbf{A}(x) \leftrightarrow \neg (\forall x \neg \mathbf{A}(x))$;

(5) $\exists x \mathbf{A}(x) \vee \exists x \mathbf{B}(x) \leftrightarrow \exists x (\mathbf{A}(x) \vee \mathbf{B}(x))$;

(6) $\forall x \mathbf{A}(x) \wedge \forall x \mathbf{B}(x) \leftrightarrow \forall x (\mathbf{A}(x) \wedge \mathbf{B}(x))$.

Il existe dans la logique des assertions une méthode générale permettant en un nombre fini d'opérations de dégager pour toute formule propositionnelle si cette dernière est identiquement vraie (méthode des tables de vérité). En logique des prédicats on ne connaît pas de méthode aussi générale permettant en un nombre fini d'opérations d'élucider pour toute formule prédicative si cette dernière est universelle ou non. Pour certains types de formules on a élaboré des méthodes semblables.

Exercices

1. Rechercher si les formules suivantes sont universelles (si non le confirmer par des exemples):

(a) $\exists x \mathrm{P}(x) \rightarrow \forall x \mathrm{P}(x)$;

(b) $\forall x \mathrm{P}(x) \rightarrow \mathrm{P}(y)$;

(c) $\mathrm{P}(y) \rightarrow \forall x \mathrm{P}(x)$;

(d) $\exists x \mathrm{Q}(x) \rightarrow \mathrm{Q}(y)$;

(e) $\forall x \exists y \mathrm{Q}(x, y) \rightarrow \exists y \forall x \mathrm{Q}(x, y)$;

(f) $\forall x \forall y \forall z (\mathrm{P}(x, y) \wedge \mathrm{P}(y, z) \rightarrow \mathrm{P}(x, z))$;

(g) $\forall x \mathrm{P}(x) \vee \forall x \mathrm{Q}(x) \leftrightarrow \exists x (\mathrm{P}(x) \wedge \mathrm{Q}(x))$;

(h) $\forall x (\mathrm{P}(x) \leftrightarrow \mathrm{Q}(x)) \rightarrow \exists (x \mathrm{P}(x) \leftrightarrow \exists x \mathrm{Q}(x))$;

(i) $\exists x \mathrm{P}(x) \wedge \exists x \mathrm{Q}(x) \rightarrow \exists x (\mathrm{P}(x) \wedge \mathrm{Q}(x))$;

(j) $\forall x (\mathrm{P}(x) \vee \mathrm{Q}(x)) \rightarrow \forall x \mathrm{P}(x) \vee \forall x \mathrm{Q}(x)$.

2. Montrer le bien-fondé de l'universalité des formules suivantes:

(a) $\forall x \mathrm{P}(x) \vee \forall x \mathrm{Q}(x) \rightarrow \forall x (\mathrm{P}(x) \vee \mathrm{Q}(x))$;

(b) $\exists x (\mathrm{P}(x) \wedge \mathrm{Q}(x)) \rightarrow \exists x \mathrm{P}(x) \wedge \exists x \mathrm{Q}(x)$;

(c) $\forall x (\mathrm{P}(x) \rightarrow \mathrm{Q}(x)) \rightarrow (\forall x \mathrm{P}(x) \rightarrow \forall x \mathrm{Q}(x))$;

(d) $\forall x (\mathrm{P}(x) \leftrightarrow \mathrm{Q}(x)) \rightarrow (\forall x \mathrm{P}(x) \leftrightarrow \forall x \mathrm{Q}(x))$;

(e) $\forall x (\mathrm{P}(x) \rightarrow \mathrm{Q}(x)) \rightarrow (\exists x \mathrm{P}(x) \rightarrow \exists x \mathrm{Q}(x))$;

(f) $\forall x \mathrm{Q}(x) \rightarrow \exists x \mathrm{Q}(x)$;

(g) $\forall x \mathrm{P}(x) \rightarrow \mathrm{P}(y)$;

(h) $\mathrm{Q}(y) \rightarrow \exists x \mathrm{Q}(x)$;

(i) $\neg \neg \forall x \mathrm{P}(x, y) \rightarrow \forall x \mathrm{P}(x, y)$;

(j) $\forall x \forall y \mathrm{P}(x, y) \leftrightarrow \forall y \forall x \mathrm{P}(x, y)$;

(k) $\exists x \exists y \mathrm{R}(x, y) \leftrightarrow \exists y \exists x \mathrm{R}(x, y)$;

(l) $\exists x \mathrm{P}(x) \wedge \exists x \mathrm{Q}(x) \leftrightarrow \exists x \exists y (\mathrm{P}(x) \wedge \mathrm{Q}(y))$;

(m) $\forall x \mathrm{R}(x) \vee \forall x \mathrm{Q}(x) \leftrightarrow \forall x \forall y (\mathrm{P}(x) \vee \mathrm{Q}(y))$;

(n) $\forall x \mathrm{Q}(x, z) \leftrightarrow \forall y \mathrm{Q}(y, z)$;

(o) $\exists x \mathrm{P}(x, z) \leftrightarrow \exists y \mathrm{P}(y, z)$;

(p) $\forall x \neg \mathrm{P}(x) \vee \forall x \mathrm{Q}(x) \leftrightarrow \exists x \mathrm{P}(x) \rightarrow \forall x \mathrm{Q}(x)$;

(r) $\exists x (\mathrm{P}(x) \rightarrow \mathrm{Q}(x)) \leftrightarrow \forall x \mathrm{P}(x) \rightarrow \exists x \mathrm{Q}(x)$.

CHAPITRE II

ENSEMBLES ET RELATIONS

§ 1. Ensembles

Notion d'ensemble. La notion d'ensemble est l'une des plus importantes en mathématiques. On entend sous le terme *ensemble* une collection d'objets (articles matériels ou notions abstraites) considérée comme un tout. On peut, par exemple, parler de l'ensemble de tous les nombres naturels, de l'ensemble de lettres d'une page, de l'ensemble de racines d'une équation donnée, etc. Les objets composant un ensemble sont appelés *éléments*. La notion d'ensemble est considérée comme intuitive, primaire, c'est-à-dire ne pouvant être réduite à d'autres notions.

Les affirmations « L'objet a est un élément de l'ensemble A », « L'objet a appartient à l'ensemble A » dont la signification est la même peuvent s'écrire de façon compacte sous la forme $a \in A$.

Si l'élément a n'appartient pas à l'ensemble A, on écrit $a \notin A$.

Le symbole $\in$ est appelé *signe d'appartenance*.

DÉFINITION. Deux ensembles A et B sont dits *égaux* et l'on écrit $A = B$ si A et B contiennent les mêmes éléments.

Ainsi, les *ensembles* A et B sont *égaux* si pour tout x $x \in A$ si et seulement si $x \in B$. Par suite, la démonstration de l'égalité de deux ensembles donnés A et B revient habituellement à la démonstration de deux affirmations: 1) pour tout x si $x \in A$, $x \in B$; 2) pour tout x si $x \in B$, $x \in A$.

On désigne fréquemment un ensemble par ses éléments mis entre accolades. C'est ainsi, par exemple, que l'ensemble composé d'éléments a, b, c est noté $\{a, b, c\}$. L'ensemble composé d'éléments $a_1, a_2, \ldots, a_n$ est désigné par $\{a_1, a_2, \ldots, a_n\}$.

Les ensembles $\{1, 2, 3\}$ et $\{3, 1, 2, 1\}$ sont égaux, car chaque élément du premier ensemble appartient au second ensemble et réciproquement. Ils sont tous deux composés de trois éléments. On se sert habituellement de la notation $\{1, 2, 3\}$.

Un ensemble peut être composé d'un seul élément. Il faut distinguer l'élément a de l'ensemble $\{a\}$ ne contenant qu'un seul élément a, car on admet l'existence d'ensembles dont les éléments constituent eux-mêmes des ensembles. Par exemple, l'ensemble

$a = \{2, 1\}$ est composé de deux éléments 2 et 1 ; l'ensemble $\{a\}$ a un seul élément a qui de son côté possède deux éléments.

Sous-ensembles.

DÉFINITION. L'ensemble A est dit *sous-ensemble* de l'ensemble B si chaque élément de l'ensemble A appartient à l'ensemble B.

Si A est un sous-ensemble de l'ensemble B, on dit de même que A est contenu dans B et l'on écrit $A \subset B$. Le symbole $\subset$ est appelé *signe d'inclusion*. Selon la définition

$$A \subset B \leftrightarrow (\text{pour chaque } x,\ x \in A \rightarrow x \in B).$$

L'ensemble A est appelé *sous-ensemble propre* de l'ensemble B si $A \subset B$ et $A \neq B$. La notation $A \subsetneq B$ signifie que A est le sous-ensemble propre de l'ensemble B.

Notons les propriétés de la relation d'inclusion qui se déduisent sans peine de la définition:

(a) la relation d'inclusion est *réflexive*, c'est-à-dire $A \subset A$ pour tout ensemble A ;

(b) la relation d'inclusion est *transitive*, c'est-à-dire que pour tous ensembles A, B, C il s'ensuit de $A \subset B$ et $B \subset C$ que $A \subset C$;

(c) la relation d'inclusion est *antisymétrique*, c'est-à-dire que pour tous ensembles A, B, C il s'ensuit de $A \subset B$ et $B \subset A$ que $A = B$.

Il découle de la propriété (c) que pour établir l'égalité des ensembles A et B il suffit de démontrer que $A \subset B$ et $B \subset A$, c'est-à-dire

$$(A = B) \leftrightarrow (A \subset B \wedge B \subset A).$$

En théorie des ensembles on adopte le principe suivant pour la séparation des sous-ensembles d'un ensemble donné avec l'office des prédicats monadiques: *pour tout ensemble A et un prédicat monadique P (x) significatif pour tous les éléments de l'ensemble A* (c'est-à-dire tel que, pour tout x de A, $P(x)$ est vrai ou bien faux) *il existe un ensemble composé exactement d'éléments de l'ensemble A pour lesquels P (x) est vrai.*

Cet ensemble est noté ainsi:

$$\{x \in A \mid P(x) \text{ est vrai}\}, \text{ ou de façon plus concise : } \{x \in A \mid P(x)\}.$$

La dernière notation se lit: « l'ensemble de tels x de A que $P(x)$ soit valable » ou « l'ensemble de tels x de A pour lesquels $P(x)$ est vrai ». Parfois pour désigner cet ensemble on se sert de la notation:

$$\{x \mid x \in A \wedge P(x)\}.$$

Si deux prédicats monadiques $P(x)$ et $Q(x)$ sont équipotents, alors, en vertu de la définition de l'égalité des ensembles, ils définissent un même sous-ensemble de l'ensemble A, c'est-à-dire que de

l'équipotence $P(x) \equiv Q(x)$ se dégage l'égalité

$$\{x \in A \mid P(x)\} = \{x \in A \mid Q(x)\}.$$

Ensemble vide. Introduisons une nouvelle notion importante.

DÉFINITION. Un ensemble qui ne contient aucun élément est appelé *ensemble vide*.

Ainsi, l'ensemble A est dit vide si pour tout x $x \notin A$. Un tel ensemble est unique. En effet, si C et D sont des ensembles vides, on a alors pour chaque x l'équivalence $x \in C \leftrightarrow x \in D$, vu que ses deux termes sont faux. Selon la définition de l'égalité des ensembles il s'ensuit que $C = D$.

L'ensemble vide unique est noté par le symbole $\varnothing$. Donc pour chaque x, $x \notin \varnothing$.

PROPOSITION 1.1. *Un ensemble vide est un sous-ensemble de tout ensemble.*

Démonstration. En effet, soit A un ensemble quelconque. Pour chaque x se vérifie l'implication $x \in \varnothing \rightarrow x \in A$, car une implication à prémisse fausse est vraie. Par conséquent, $\varnothing \subset A$. □

Opérations sur les ensembles. Etudions les opérations sur des ensembles permettant d'obtenir à partir de deux ensembles quelconques des ensembles nouveaux.

DÉFINITION. On appelle *réunion de deux ensembles* A et B l'ensemble composé des seuls éléments appartenant à l'un au moins des ensembles A et B et rien que d'eux.

Un tel ensemble existe toujours.

De la définition de l'égalité de deux ensembles il suit que pour tous ensembles A et B il existe un ensemble unique constituant leur réunion. Et de fait, s'il existait deux tels ensembles C et D, ils seraient composés des mêmes éléments et, partant, devraient coïncider. Cet ensemble unique, réunion des ensembles A et B, est noté $A \cup B$. Ainsi, par définition,

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

Par conséquent, pour un x quelconque on a l'équivalence

$$x \in A \cup B \leftrightarrow x \in A \vee x \in B.$$

De la définition de la réunion d'ensembles il suit également que $A \subset A \cup B$ et $B \subset A \cup B$.

Exemple. Si $A = \{1, 9, 18\}$ et $B = \{1, 5, 9\}$, alors $A \cup B = \{1, 5, 9, 18\}$.

DÉFINITION. On appelle *intersection des ensembles* A et B l'ensemble composé des éléments communs à A et B et rien que d'eux.

Un tel ensemble existe toujours.

Pour deux ensembles quelconques A et B il existe un ensemble unique constituant leur intersection. Et de fait, s'il existait deux

tels ensembles C et D, ils contiendraient alors les mêmes éléments et, par suite, coïncideraient. L'intersection des ensembles A et B est notée par $A \cap B$. Donc, par définition

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

Par conséquent, pour un x quelconque on a l'équivalence

$$x \in A \cap B \leftrightarrow x \in A \wedge x \in B.$$

Il s'ensuit de la définition de l'intersection des ensembles que

$$A \cap B \subset A \text{ et } A \cap B \subset B.$$

Exemple. Si $A = \{1/2, 2/3, 5/6\}$, $B = \{1, 3/2, 1/2\}$, alors $A \cap B = \{1/2\}$.

DÉFINITION. On appelle *différence des ensembles* A et B l'ensemble constitué d'éléments de l'ensemble A n'appartenant pas à l'ensemble B et rien que d'eux.

Pour des ensembles quelconques A et B on a toujours un tel ensemble et il est unique. La différence des ensembles A et B est notée $A \setminus B$. Donc, par définition,

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}.$$

Par conséquent, pour un x quelconque on a l'équivalence

$$x \in A \setminus B \leftrightarrow x \in A \wedge x \notin B.$$

Exemple. Si $A = \{6, 9, 12, 13\}$, $B = \{6, 9, 10\}$, alors $A \setminus B = \{12, 13\}$.

THÉORÈME 1.2. *Pour des ensembles quelconques A et B les trois relations suivantes sont équivalentes*:

$$\text{(a) } A \subset B; \quad \text{(b) } A \cup B = B; \quad \text{(c) } A \cap B = A.$$

Démonstration. (a) $\rightarrow$ (b). Chaque élément de l'ensemble $A \cup B$ appartient à A ou B et, en vertu de (a), est un élément de l'ensemble B, c'est-à-dire $A \cup B \subset B$. En outre, $B \subset A \cup B$; par conséquent, $A \cup B = B$;

(a) $\rightarrow$ (c). En vertu de (a) chaque élément de l'ensemble A est un élément commun de A et B, c'est-à-dire $A \subset A \cap B$. De plus $A \cap B \subset A$; par conséquent, $A \cap B = A$;

(b) $\rightarrow$ (c). On a $A \subset A \cup B$ et, en vertu de (b), $A \cup B \subset B$, aussi $A \subset B$. Comme (a) $\rightarrow$ (c), on a l'égalité (c);

(c) $\rightarrow$ (a). En vertu de (c) $A \subset A \cap B$. Mais on a aussi $A \cap B \subset B$; par conséquent, $A \subset B$. □

Propriétés principales des opérations sur des ensembles. Les opérations réunion et intersection sur des ensembles possèdent une série de propriétés. On passera en revue les principales propriétés de ces opérations.

THÉORÈME 1.3. *On a pour des ensembles quelconques A, B et C*

(1) $A \cup A = A$ *idempotence de la réunion;*

(2) $A \cap A = A$ *idempotence de l'intersection;*

(3) $A \cup B = B \cup A$ *commutativité de la réunion;*

(4) $A \cap B = B \cap A$ *commutativité de l'intersection;*

(5) $A \cup (B \cup C) = (A \cup B) \cup C$ *associativité de la réunion;*

(6) $A \cap (B \cap C) = (A \cap B) \cap C$ *associativité de l'intersection;*

(7) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *distributivité de la réunion relativement à l'intersection;*

(8) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *distributivité de l'intersection relativement à la réunion.*

D é m o n s t r a t i o n. Les quatre premières propriétés d'idempotence et de commutativité se déduisent sans peine de la définition des opérations de réunion et d'intersection. Pour démontrer la propriété d'associativité (5) il suffit de noter que $A \cup (B \cup C)$ est un ensemble d'éléments appartenant à l'ensemble A ou à l'ensemble B, ou à l'ensemble C, quant à l'ensemble $(A \cup B) \cup C$, il est composé des mêmes éléments. De façon analogue se démontre la propriété (6).

Démontrons la propriété (7). Soient

$$D = A \cup (B \cap C), \qquad E = (A \cup B) \cap (A \cup C).$$

Il faut démontrer que les ensembles D et E sont égaux, c'est-à-dire: (a) si $x \in D$, alors $x \in E$; (b) si $x \in E$, alors $x \in D$.

Soit $x \in A \cup (B \cap C)$. Deux cas se présentent:

$$(\mathrm{a}_1)\ x \in A \quad \text{et} \quad (\mathrm{a}_2)\ x \in B \cap C.$$

Si (a_1) $x \in A \cup B$ et $x \in A \cup C$; par conséquent, $x \in E$. Si (a_2) $x \in B$ et $x \in C$, de sorte que $x \in A \cup B$ et $x \in A \cup C$; par conséquent, $x \in E$.

Supposons maintenant que $x \in E$, c'est-à-dire que $x \in (A \cup B) \cap \cap (A \cup C)$, alors

$$x \in A \cup B \quad \text{et} \quad x \in A \cup C.$$

De plus, si $x \notin A$, alors $x \in B$ et $x \in C$, de sorte que $x \in B \cap C$; par conséquent, $x \in A \cup (B \cap C)$. Si par contre $x \in A$, alors $x \in A \cup \cup (B \cap C)$, c'est-à-dire $x \in D$. De (a) et (b) se déduit l'égalité (5).

La propriété de distributivité (8) se démontre de façon analogue. □

Ensemble universel. Complémentaire d'un ensemble. Dans nombre d'applications de la théorie des ensembles on ne considère que les ensembles inclus dans un certain ensemble fixé. Par exemple, en

géométrie on a affaire à des ensembles de points d'un espace donné, en arithmétique élémentaire à des sous-ensembles d'ensemble de tous les entiers.

Dans la suite de l'exposé les lettres A, B, . . . désigneront toujours les ensembles inclus dans un certain ensemble fixé qu'on appellera *ensemble universel* en le notant U. On considère donc que pour tout ensemble A on a $A \subset U$. Par conséquent, pour chaque ensemble A :

(1) $A \cup U = U, \quad A \cap U = A.$

DÉFINITION. L'ensemble $U \setminus A$ est appelé *complémentaire de l'ensemble* A et est noté A' (ou $\bar{A}$). Le complémentaire $U \setminus A'$ de l'ensemble A' est noté A'' (ou $\bar{\bar{A}}$).

On voit sans peine que

(2) $A \cup A' = U, \quad A \cap A' = \varnothing.$

PROPOSITION 1.4. *Pour tout ensemble* A

(3) $A'' = A$ (loi d'involution).

On laisse au lecteur le soin d'esquisser la démonstration.

PROPOSITION 1.5. *Si* $A \subset B$, *alors* $B' \subset A'$.

Démonstration. Soit $A \subset B$. On doit démontrer que pour tout x de U si $x \in B'$, on a $x \in A'$. En effet, si $x \in B'$, alors $x \notin B$. Compte tenu de la condition $A \subset B$, on conclut que $x \notin A$ et $x \in A'$. □

THÉORÈME 1.6. *On a les identités suivantes*:

(4) $(A \cup B)' = A' \cap B'$
(5) $(A \cap B)' = A' \cup B'$
(*lois de de Morgan appliquées aux ensembles*).

Démonstration. Montrons que pour tout x on a

(6) $x \in (A \cup B)' \leftrightarrow x \in A' \cap B'.$

De fait, $x \in (A \cup B)'$ si et seulement si $x \notin A \cup B$. Mais $x \notin A \cup B$ si et seulement si $x \notin A$ et $x \notin B$, c'est-à-dire si $x \in A'$ et $x \in B'$ et, par suite, $x \in A' \cap B'$.

L'identité (5) se démontre de la façon suivante. En utilisant l'identité (4) et la loi d'involution, on obtient

$$(A' \cup B')' = A'' \cap B'' = A \cap B.$$

Par conséquent,

$$(A \cap B)' = (A' \cup B')'' = A' \cup B',$$

c'est-à-dire que l'identité (5) est vraie. □

Diagramme d'Euler-Venn. Pour la représentation graphique des ensembles et de leurs propriétés on utilise les diagrammes d'Euler appelés également diagrammes de Venn. Un ensemble est représenté par un cercle (ou par toute autre figure

fermée) sur un plan et est sensé constituer l'ensemble des points du cercle. Si l'on représente par des cercles les ensembles A et B, les ensembles $A \cap B$ et $A \cup B$ correspondront aux parties hachurées

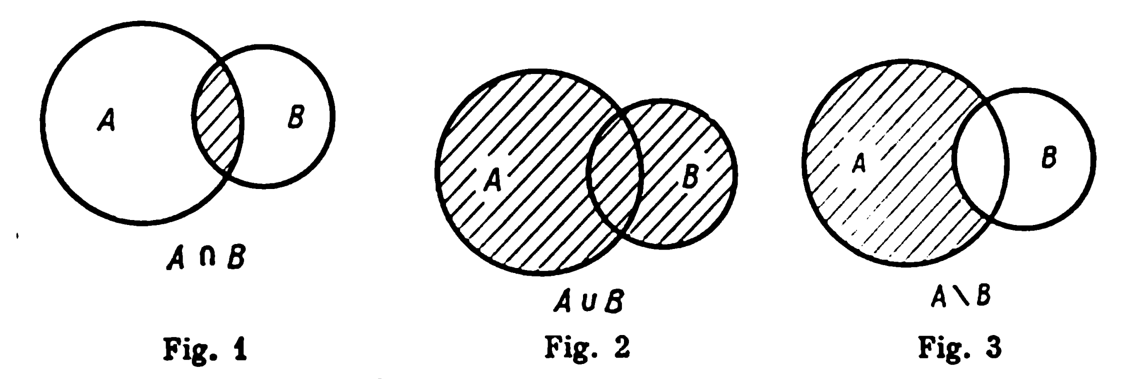


Fig. 1 Fig. 2 Fig. 3

(fig. 1 et 2). Les ensembles $A \setminus B$ et $B \setminus A$ seront rendus respectivement par les diagrammes des figures 3 et 4. La relation $A \subset B$ est représentée sur la figure 5.

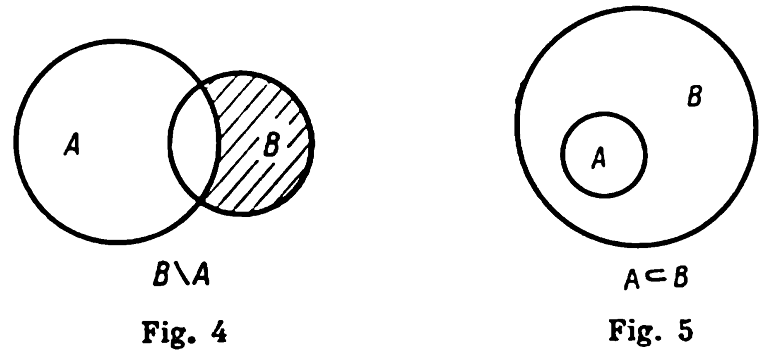


Fig. 4 Fig. 5

L'ensemble universel U est figuré par l'ensemble des points d'un certain rectangle. Le complémentaire A' de l'ensemble A jusqu'à U

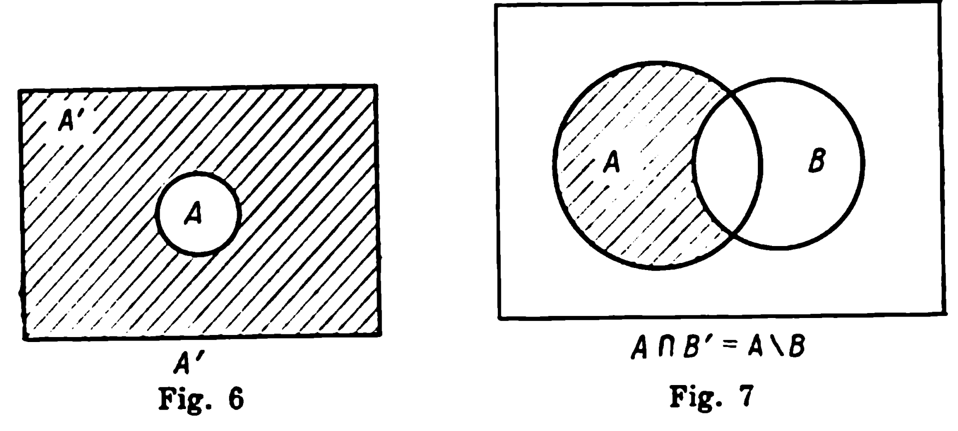


Fig. 6 Fig. 7

est la partie hachurée du rectangle (fig. 6) se trouvant à l'extérieur du cercle-image de l'ensemble A. L'égalité $A \setminus B = A \cap B'$ est illustrée sur la figure 7.

Exercices

1. Démontrer les identités suivantes:

(a) $A \setminus B = A \cap B'$;
(b) $A \setminus (A \setminus B) = A \cap B$;
(c) $B \cup (A \setminus B) = A \cup B$;
(d) $B \cap (A \setminus B) = \varnothing$;
(e) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
(f) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

Représenter ces identités au moyen des diagrammes d'Euler-Venn.

2. Montrer par des exemples que les formules suivantes ne sont pas toujours vraies:

(a) $(A \cup B) \setminus B = A$; (b) $(A \setminus B) \cup B = A$.

3. Démontrer les affirmations suivantes:

(a) $B \subset A \to (A \setminus B) \cup B = A$;
(b) $A \subset B \equiv A \cap B = A$;
(c) $A \subset B \equiv A \cup B = A$;
(d) $A \cap B = \varnothing \to (A \cup B) \setminus B = A$;
(e) $A \subset B \to A \setminus C \subset B \setminus C$;
(f) $A \subset B \to A \cap C \subset B \cap C$;
(g) $A \subset B \to A \cup C \subset B \cup C$;
(h) $B \subset A \wedge C = A \setminus B \to A = B \cup C$;
(i) $A \not\subset B \wedge B \cap C = \varnothing \to A \cup C \not\subset B \cup C$;
(k) $C = A \setminus B \to B \cap C = \varnothing$;
(l) $A \not\subset B \to A \setminus B \neq \varnothing$;
(m) $B \cap C = \varnothing \wedge A \cap C \neq \varnothing \to A \setminus B \neq \varnothing$;
(n) $A \subset C \to A \cup (B \cap C) = (A \cup B) \cap C$.

Illustrer ces affirmations au moyen des diagrammes d'Euler-Venn.

4. Démontrer les équipotences suivantes:

(a) $A \cup B = \varnothing \equiv A = \varnothing \wedge B = \varnothing$;
(b) $A \setminus B = A \equiv B \setminus A = B$;
(c) $A \cup B = A \setminus B \equiv B = \varnothing$;
(d) $A \setminus B = A \cap B \equiv A = \varnothing$;
(e) $A \cup B \subset C \equiv A \subset C \wedge B \subset C$;
(f) $C \subset A \cap B \equiv C \subset A \wedge C \subset B$;
(g) $A \subset B \cup C \equiv A \setminus B \subset C$;
(h) $A \cap B = A \cup B \equiv A = B$;
(i) $A \subset B \subset C \equiv A \cup B = B \cap C$.

5. Soient A et B des ensembles finis. Démontrer que $n(A \cap B) = n(A) + n(B) - n(A \cap B)$, où $n(M)$ est le nombre d'éléments de l'ensemble M.

6. Démontrer que l'ensemble composé de n éléments possède 2^n sous-ensembles différents.

7. Montrer que pour $m < n$ l'ensemble composé de n éléments possède $\frac{n!}{(n-m)!(m!)}$ sous-ensembles différents à m éléments (où $m! = 1 \cdot 2 \ldots m$).

8. Soient $A(x)$ et $B(x)$ des prédicats monadiques et U le domaine des valeurs spécifiées de la variable x. Démontrer qu'alors:

$\{x \mid A(x) \vee B(x)\} = \{x \mid A(x)\} \cup \{x \mid B(x)\}$;

$\{x \mid A(x) \wedge B(x)\} = \{x \mid A(x)\} \cap \{x \mid B(x)\}$;

$\{x \mid \neg A(x)\} = U \setminus \{x \mid A(x)\} = \{x \mid A(x)\}'$;

$\{x \mid A(x) \rightarrow B(x)\} = \{x \mid A(x)\}' \cup \{x \mid B(x)\}$;

$\{x \mid A(x) \leftrightarrow B(x)\} = (\{x \mid A(x)\}' \cap \{x \mid B(x)\}') \cup (\{x \mid A(x)\} \cap$
$\cap \{x \mid B(x)\})$.

§ 2. Relations binaires

Produit direct d'ensembles. Soient donnés des objets quelconques a et b. Si $a \neq b$, l'ensemble $\{a, b\}$ est appelé *couple non ordonné d'objets* a et b. Notons qu'on a toujours $\{a, b\} = \{b, a\}$.

Introduisons une nouvelle notion élémentaire, la notion de couple ordonné. Associons à deux objets a et b un nouveau objet constitué par leur couple ordonné $\langle a, b\rangle$.

DÉFINITION. Les couples ordonnés $\langle a, b\rangle$ et $\langle c, d\rangle$ sont dits *égaux* et l'on écrit $\langle a, b\rangle = \langle c, d\rangle$ si et seulement si $a = c$ et $b = d$.

En particulier, $\langle a, b\rangle = \langle b, a\rangle$ si et seulement si $a = b$.

Dans la suite on dira souvent « couple $\langle a, b\rangle$ » au lieu de « couple ordonné $\langle a, b\rangle$ ». L'élément a est appelé *premier élément du couple* $\langle a, b\rangle$, tandis que b est le *second élément du couple*.

DÉFINITION. On appelle *produit direct des ensembles* A et B l'ensemble de tous les couples ordonnés $\langle x, y\rangle$ tels que $x \in A$ et $y \in B$. On note cet ensemble $A \times B$.

Donc,

$$A \times B = \{\langle x, y\rangle \mid x \in A \wedge y \in B\}.$$

Exemple. Soient $A = \{0, 1, 2\}$ et $B = \{3, 5\}$. On a alors

$$A \times B = \{\langle 0,3\rangle, \langle 0,5\rangle, \langle 1,3\rangle, \langle 1,5\rangle, \langle 2,3\rangle, \langle 2,5\rangle\};$$

$$B \times A = \{\langle 3,0\rangle, \langle 5,0\rangle, \langle 3,1\rangle, \langle 5,1\rangle, \langle 3,2\rangle, \langle 5,3\rangle\};$$

$$A \times A = \{\langle 0,0\rangle, \langle 0,1\rangle, \langle 0,2\rangle, \langle 1,1\rangle, \langle 1,0\rangle, \langle 1,2\rangle, \langle 2,0\rangle, \langle 2,1\rangle, \langle 2,2\rangle\};$$

$$B \times B = \{\langle 3,3\rangle, \langle 3,5\rangle, \langle 5,5\rangle, \langle 5,3\rangle\}.$$

La notion généralisée de couple ordonné est la notion de cortège (jeu ordonné) de n objets. Le cortège de n objets $a_1, \ldots, a_n$ est noté $\langle a_1, \ldots, a_n\rangle$.

DÉFINITION. Deux cortèges $\langle a_1, \ldots, a_n\rangle$ et $\langle b_1, \ldots, b_n\rangle$ sont dits *égaux* et l'on écrit $\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle$ si et seulement si $a_1 = b_1, \ldots, a_n = b_n$.

Les cortèges de trois objets sont également appelés *triplets ordonnés*. On appelle *produit direct de trois ensembles* A, B et C l'ensemble de tous les triplets ordonnés $\langle x, y, z\rangle$ tels que $x \in A$, $y \in B$ et $z \in C$.

Cet ensemble est noté $A \times B \times C$; donc,

$$A \times B \times C = \{\langle x, y, z\rangle \mid x \in A, y \in B, z \in C\}.$$

Soient A un ensemble non vide et n un entier positif. On note A^n l'ensemble des cortèges $\langle x_1, \ldots, x_n\rangle$ d'éléments de A, c'est-à-dire,

$$A^n = \{\langle x_1, \ldots, x_n\rangle \mid x_1 \in A, \ldots, x_n \in A\}.$$

On admettra de même que $A^1 = A$. L'ensemble A^n est appelé n-uple produit direct de l'ensemble A ou puissance n-ième de l'ensemble A. En particulier, $A^2 = A \times A$ et $A^3 = A \times A \times A$.

DÉFINITION. On appelle *produit direct* de n ensembles $A_1, \ldots, A_n$ l'ensemble des cortèges de longueur n $\langle x_1, \ldots, x_n\rangle$ tels que $x_1 \in A_1, \ldots, x_n \in A_n$.

Le produit direct des ensembles $A_1, \ldots, A_n$ est noté par le symbole $A_1 \times A_2 \times \ldots \times A_n$; donc,

$$A_1 \times \ldots \times A_n = \{\langle x_1, \ldots, x_n\rangle \mid x_1 \in A_1, \ldots, x_n \in A_n\}.$$

Relations binaires. C'est une des notions essentielles de la théorie des ensembles.

DÉFINITION. On appelle *relation binaire* tout ensemble de couples ordonnés.

Il s'ensuit de la définition qu'un sous-ensemble quelconque du produit direct de deux ensembles est une relation binaire.

Si R est une relation binaire et $\langle x, y\rangle \in R$, on dit que x et y *sont liés par la relation R* ou bien que l'*élément x est en relation R avec y* ou encore que pour x et y *est remplie la relation R*. Au lieu de $\langle x, y\rangle \in R$ on utilise souvent une notation plus simple:

$$xRy,$$

employée également pour noter l'affirmation « les éléments x et y sont liés par la relation R ».

DÉFINITION. L'ensemble des premiers éléments des couples de R est appelé *domaine (ensemble) de définition de la relation R* et est noté Dom R:

$$\text{Dom } R = \{x \mid \exists\, y\, (\langle x, y\rangle \in R)\}.$$

L'ensemble des seconds éléments des couples de R est appelé *domaine de valeurs de la relation R* et est noté Im R:

$$\text{Im } R = \{y \mid \exists\, x\, (\langle x, y\rangle \in R)\}.$$

DÉFINITION. L'ensemble Dom $R \cup$ Im R est appelé *domaine de la relation R*.

On voit sans peine que

$$R \subset \text{Dom } R \times \text{Im } R.$$

Si $R \subset A \times B$, on dit que R est la *relation entre les éléments des ensembles* A et B ou que R *est défini sur un couple d'ensembles* A et B. Si $A \subset C$ et $B \subset D$, on a $R \subset C \times D$, c'est-à-dire que R est également la relation entre les éléments des ensembles C et D. Si $R \subset \subset A \times B$, alors Dom $R \subset A$ et Im $R \subset B$. Chaque relation R est ainsi une relation entre les éléments des ensembles Dom R et Im R.

DÉFINITION. Si $R \subset A \times A$, on dit que R est *une relation binaire* sur l'ensemble A.

Il est clair que chaque relation binaire R est une relation sur le domaine de la relation R.

DÉFINITION. Les relations binaires R et S sont dites *égales* si et seulement si $\langle x, y\rangle \in S$ pour tous x, y $\langle x, y\rangle \in R$, c'est-à-dire si R et S sont égaux en tant qu'ensembles.

DÉFINITION. Soient R et S des relations binaires. L'ensemble de tous les couples $\langle x, y\rangle$ tels que pour un certain z $\langle x, z\rangle \in S$ et $\langle z, y\rangle \in R$ est appelé *composition* (ou *superposition*) *des relations* S et R et est noté $R \circ S$.

Par définition, on a

$$R \circ S = \{\langle x, y\rangle \mid \exists z\, (xSz \wedge zRy)\}.$$

Exemple. Si $S = \{\langle 1, 2\rangle, \langle 2, 4\rangle, \langle 3, 6\rangle\}$, $R = \{\langle 1, 3\rangle, \langle 2, 6\rangle, \langle 3, 9\rangle, \langle 4, 12\rangle\}$, alors $R \circ S = \{\langle 1, 6\rangle, \langle 2, 12\rangle\}$.

DÉFINITION. On appelle *inversion* de la relation binaire R l'ensemble de tous les couples ordonnés $\langle x, y\rangle$ tels que $\langle y, x\rangle \in R$.

L'inversion de la relation R est notée $R^{\smile}$. Donc, par définition,

$$R^{\smile} = \{\langle x, y\rangle \mid \langle y, x\rangle \in R\}.$$

Exemple. Si $R = \{\langle 2, 5\rangle, \langle 8, 15\rangle, \langle 4, 1\rangle\}$, alors $R^{\smile} = \{\langle 5, 2\rangle, \langle 15, 8\rangle, \langle 1, 4\rangle\}$.

PROPOSITION 2.1. *Si R est une relation binaire quelconque*, on a

$$\text{(a) Dom}\,(R^{\smile}) = \text{Im}\,R, \quad \text{(b) Im}\,(R^{\smile}) = \text{Dom}\,R, \quad \text{(c) } (R^{\smile})^{\smile} = R,$$

c'est-à-dire que si $R^{\smile}$ est une inversion de R, réciproquement, R est l'inversion de $R^{\smile}$.

Cette proposition se déduit directement de la définition de l'inversion $R^{\smile}$ de la relation R.

DÉFINITION. La relation R est dite *restriction* de la relation S, et S *extension* de R, si $R \subset S$.

DÉFINITION. La relation binaire R est appelée *restriction de la relation* S par l'ensemble A, si $R = (A \times A) \cap S$.

Si la relation binaire R est une restriction de la relation S par l'ensemble A, R est réciproquement la restriction de S et Dom $R \subset A$.

THÉORÈME 2.2. *La composition des relations est douée de la propriété d'associativité, c'est-à-dire pour toutes relations binaires R, S,*

T *on a:*

(1) $(R \circ S) \circ T = R \circ (S \circ T)$.

Démonstration. Pour tous x et y on a

$$
\begin{aligned}
x (R \circ S) \circ T y &\leftrightarrow \exists z\, (xTz \wedge zR \circ Sy)\\
&\leftrightarrow \exists z \exists t\, (xTz \wedge zSt \wedge tRy)\\
&\leftrightarrow \exists t \exists z\, (xTz \wedge zSt \wedge tRy)\\
&\leftrightarrow \exists t\, [\exists z\, (xTz \wedge zSt) \wedge tRy]\\
&\leftrightarrow \exists t\, [xS \circ Tt \wedge tRy]\\
&\leftrightarrow xR \circ (S \circ T)\, y.
\end{aligned}
$$

Par conséquent, l'égalité (1) est vraie pour toutes relations binaires R, S et T. □

THÉORÈME 2.3. *Pour toutes relations binaires* R *et* S $(R \circ S)^{\smile} = S^{\smile} \circ R^{\smile}$.

Démonstration. Pour tous x et y on a

$$
\begin{aligned}
x (R \circ S)^{\smile} y &\leftrightarrow yR \circ Sx\\
&\leftrightarrow \exists z\, (ySz \wedge zRx)\\
&\leftrightarrow \exists z\, (xR^{\smile}z \wedge zS^{\smile}y)\\
&\leftrightarrow xS^{\smile} \circ R^{\smile}y.
\end{aligned}
$$

Par conséquent, $(R \circ S)^{\smile} = S^{\smile} \circ R^{\smile}$ pour toutes relations binaires R et S. □

Relations n-aires. La notion généralisée de la relation binaire est la notion de relation n-aire.

DÉFINITION. On appelle *relation n-aire* ($n \geqslant 1$) tout ensemble des cortèges de longueur n (c'est-à-dire un ensemble quelconque de jeux ordonnés de n objets).

Donc une relation n-aire est un sous-ensemble quelconque d'un produit direct de n ensembles.

Une relation à deux places est également appelée *relation binaire*, et une relation à trois places *relation ternaire*. La relation ternaire est constituée par tout ensemble de triplets ordonnés, c'est-à-dire tout sous-ensemble du produit direct de trois ensembles.

DÉFINITION. Soit A^n la n-ième puissance d'un ensemble non vide A, $n \geqslant 1$. Tout sous-ensemble de l'ensemble A^n est appelé *relation n-aire sur l'ensemble* A, et le nombre n *le rang de la relation.*

En particulier, tout sous-ensemble de l'ensemble A est une relation à une place (singulaire) sur A ; une relation à trois places (ternaire) sur A est constituée par tout sous-ensemble de l'ensemble A^3, c'est-à-dire tout ensemble de triplets ordonnés d'éléments de l'ensemble A.

Soit $A(x_1, \ldots, x_n)$ un prédicat n-aire quelconque à variables libres $x_1, \ldots, x_n$. On peut lui associer une relation n-aire

$$R = \{\langle x_1, \ldots, x_n\rangle \mid A(x_1, \ldots, x_n)\}.$$

La relation R est appelée *graphe du prédicat* $A(x_1, \ldots, x_n)$.

Représentation des relations binaires par des graphes. On appelle *graphe* une figure plane composée d'un nombre fini de points (des sommets du graphe) et de lignes joignant certains sommets. Une ligne joignant deux sommets quelconques du graphe est appelée *arête* du graphe. Les lignes peuvent être droites ou courbes. Les points d'intersection de certaines arêtes du graphe peuvent ne pas constituer des sommets de ce dernier. Le graphe indiquant par des flèches la direction de ses arêtes est appelé *graphe orienté*.

Il existe un procédé fort simple de représentation par des graphes orientés des relations binaires sur des ensembles finis. Soient A un ensemble fini non vide et R la relation binaire sur A, c'est-à-dire $R \subset A \times A$. Représentons les éléments de l'ensemble A par des points sur un plan. A chaque couple $\langle a, b\rangle$ de R pour $a \neq b$ associons une arête orientée (fig. 8) dirigée du point a vers le point b. Au couple $\langle a, a\rangle$ de R associons un lacet (fig. 9) avec un sens fixé de mouvement (par exemple, toujours dans le sens inverse des aiguilles d'une montre). Ainsi, à une relation binaire R est associée la figure géométrique suivante : des points du plan représentant les éléments de l'ensemble Dom $R \cup$ Im R et des arêtes orientées, c'est-à-dire qu'à chaque couple $\langle a, b\rangle$ de R on fait correspondre une arête orientée, dirigée du point a vers le point b, ou un lacet, si $a = b$. Cette figure géométrique porte le nom de *graphe orienté de la relation* R ou, tout simplement, *graphe de la relation* R.

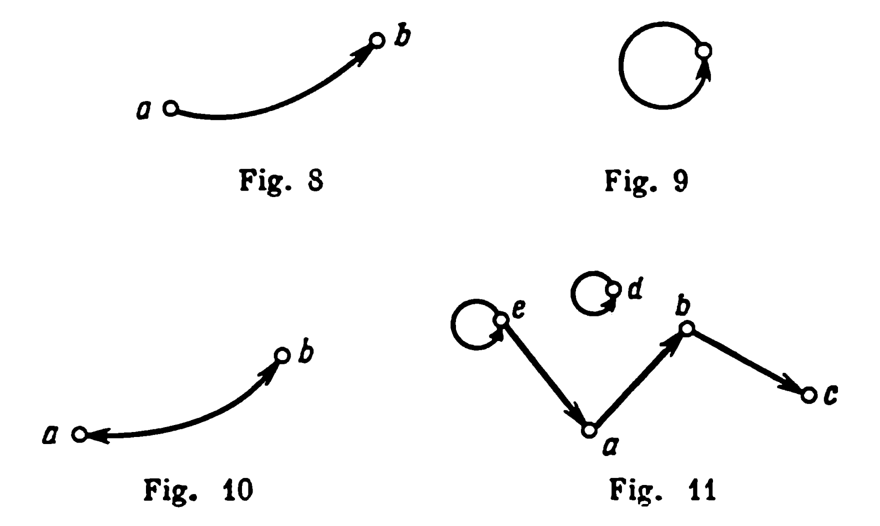


Fig. 8 Fig. 9

Fig. 10 Fig. 11

Si la relation R comprend le couple $\langle a, b\rangle$ et le couple $\langle b, a\rangle$, le graphe de la relation R possède alors deux arêtes de sommets a et b

de sens opposés. Dans ce cas les deux arêtes sont remplacées par une seule munie de deux flèches (fig. 10).

L'arête à deux flèches est dite *non orientée.*

Chaque relation binaire sur un ensemble fini peut être représentée par un graphe orienté. Inversement, *chaque graphe orienté est la représentation d'une relation binaire sur l'ensemble de ses sommets.*

Exemple. La figure 11 représente le graphe de la relation

$$R = \{\langle a, b\rangle, \langle b, c\rangle, \langle d, d\rangle, \langle e, a\rangle, \langle e, e\rangle\}.$$

Exercices

1. Montrer que pour tous éléments a, b, c, d (pas forcément différents) $\{a, b\} = \{c, d\}$ si et seulement si $a = c$ et $b = d$ ou $a = d$ et $b = c$.

2. Montrer que pour tous éléments a, b, c, d $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ si et seulement si $a = c$ et $b = d$.

Remarque. En vertu de ce fait, le couple ordonné $\langle a, b\rangle$ est souvent défini en théorie des ensembles en tant que l'ensemble $\{\{a\}, \{a, b\}\}$.

3. Montrer que $\langle\langle a, b\rangle, c\rangle = \langle\langle d, e\rangle, f\rangle$ si et seulement si $a = d$, $b = e$, $c = f$.

4. Démontrer que pour tous ensembles A, B, C, D:

(a) $\text{Dom}\,(A \times B) = A$;

(b) $\text{Im}\,(A \times B) = B$;

(c) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$;

(d) $(A \cap B) \times C = (A \times C) \cap (B \times C)$;

(e) $A \times (B \cap C) = (A \times B) \cap (A \times C)$;

(f) $(B \cup C) \times A = (B \times A) \cup (C \times A)$;

(g) $(A \times B = \varnothing) \equiv (A = \varnothing \vee B = \varnothing)$;

(h) $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$.

5. Montrer par des exemples que les égalités ci-dessous sont vraies pour tous ensembles A, B et C:

(a) $A \times B = B \times A$;

(b) $A \times (B \times C) = (A \times B) \times C$.

6. Démontrer que pour toutes relations binaires R, S, T on a:

(a) $(\text{Dom}\,(R) = \varnothing) \equiv (R = \varnothing) \equiv (\text{Im}\,(R) = \varnothing)$;

(b) $\text{Dom}\,(R^{\smile}) = \text{Im}\,(R)$;

(c) $\text{Im}\,(R^{\smile}) = \text{Dom}\,(R^{\smile})$;

(d) $(R^{\smile})^{\smile} = R$;

(e) $(R \circ S)^{\smile} = S^{\smile} \circ R^{\smile}$;

(f) $\text{Dom}\,(R \circ S) \subset \text{Dom}\,S$;

(g) $\text{Im}\,(R \circ S) \subset \text{Im}\,R$.

7. Montrer par un exemple qu'une composition de relations binaires n'est pas commutative.

8. Chercher Dom (R), Im (R), $R^{\smile}$, $R \circ R$, $R \circ R^{\smile}$, $R^{\smile} \circ R$ pour les relations suivantes:

(a) $R = \{\langle x, y\rangle \mid x, y \in \mathrm{N}$ et x divise $y\}$;

(b) $R = \{\langle x, y\rangle \mid x, y \in \mathrm{N}$ et y divise $x\}$;

(c) $R = \{\langle x, y\rangle \mid x, y \in \mathrm{Q}$ et $x + y \leqslant 0\}$, où Q est l'ensemble de tous les nombres rationnels;

(d) $R = \{\langle x, y\rangle \mid x, y \in \mathrm{Q}$ et $2x \leqslant 3y\}$.

§ 3. Fonctions

Notion de fonction (d'application). Une des notions essentielles des mathématiques est la notion de fonction.

DÉFINITION. On appelle *fonction* (*application*) la relation binaire f si pour tous x, y, z il s'ensuit de $\langle x, y\rangle \in f$ et $\langle x, z\rangle \in f$ que $y = z$.

Autrement dit, la relation f est appelée fonction si pour tout x du domaine de définition de la relation f il existe un y unique tel que $\langle x, y\rangle \in f$. Cet élément unique y est noté $f(x)$ et appelé *valeur de la fonction* f pour l'argument x. Si $\langle x, y\rangle \in f$ on se sert de la notation usuelle $y = f(x)$, ainsi que de la notation

$$f\colon x \mapsto y.$$

On appelle *domaine de définition de la fonction* f l'ensemble

$$\mathrm{Dom}\, f = \{x \mid \exists y\, (\langle x, y\rangle \in f)\}.$$

On appelle *domaine des valeurs de la fonction* f l'ensemble

$$\mathrm{Im}\, f = \{y \mid \exists x\, (\langle x, y\rangle \in f)\}.$$

Deux fonctions f et g sont dites *égales* (on écrit $f = g$) si f et g sont égaux en tant qu'ensembles, c'est-à-dire pour tous x, y $\langle x, y\rangle \in f$ si et seulement si $\langle x, y\rangle \in g$. Par conséquent, les fonctions f et g sont égales si et seulement si Dom f = Dom g et $f(x) = g(x)$ pour chaque x de Dom f.

Les fonctions sont également appelées *applications*. Si la fonction f est donnée sur le couple d'ensembles A et B, c'est-à-dire si $f \subset A \times B$, on dit que f est l'application de A dans B. Si de plus $A = \mathrm{Dom}\, f$ et $\mathrm{Im}\, f \subset B$, on dit que f est l'*application de l'ensemble* A dans B et l'on note

$$f\colon A \to B \quad \text{ou} \quad A \xrightarrow[f]{} B.$$

Si $A = \mathrm{Dom}\, f$ et $B = \mathrm{Im}\, f$, on dit que f est l'*application de l'ensemble* A *sur* B.

L'ensemble de toutes les applications de A dans B est désigné par le symbole B^A.

On appelle *image de l'ensemble* C par application f l'ensemble

$$f(C) = \{f(x) \mid x \in C\}.$$

On montre sans peine que pour tout ensemble C et toute application f

$$f(C) = f(C \cap \mathrm{Dom}\, f).$$

L'*image anticipée de l'ensemble* M par application f est l'ensemble

$$f^{\smile}(M) = \{x \in \mathrm{Dom}\, f \mid f(x) \in M\},$$

c'est-à-dire l'ensemble de tous les éléments x du domaine de définition de la fonction f pour lesquels $f(x) \in M$. On vérifie sans peine que pour un ensemble quelconque M et une application quelconque f, il vient

$$f^{\smile}(M) = f^{\smile}(M \cap \mathrm{Im}\, f).$$

On a vu qu'une relation binaire peut être donnée sous forme de graphe d'une condition à deux places (d'un prédicat). Une fonction peut également être donnée par une condition à deux places. Soit $A(x, y)$ la condition à deux places imposée à x et y, telle qu'il n'existe pas deux couples ordonnés satisfaisant à cette condition qui auraient des premiers éléments identiques et des seconds différents. Dans ce cas le graphe de la condition $A(x, y)$, c'est-à-dire l'ensemble $\{\langle x, y\rangle \mid A(x, y)\}$, est une fonction.

C'est ainsi, par exemple, que la fonction définie par la condition $x^2 - y = 1$ sur l'ensemble $\mathbf{Z}$ des entiers peut être présentée comme l'ensemble

$$f = \{\langle x, y\rangle \mid x, \quad y \in \mathbf{Z} \quad \text{et} \quad x^2 - y = 1\},$$

ou par

$$f = \{\langle x, y\rangle \mid x, \quad y \in \mathbf{Z} \quad \text{et} \quad y = x^2 - 1\},$$

ou encore sous la forme suivante:

$$f = \{\langle x, \quad x^2 - 1\rangle \mid x, \quad y \in \mathbf{Z}\}.$$

La fonction dont le domaine de définition est composé de couples ordonnés est appelée *fonction de deux variables*. La fonction dont le domaine de définition est composé de triplets ordonnés est appelée *fonction de trois variables*. Si f est une fonction de deux variables on écrit alors habituellement $f(x, y)$ au lieu de $f(\langle x, y\rangle)$. Si f est une fonction de trois variables on écrit $f(x, y, z)$ à la place de $f(\langle x, y, z\rangle)$.

Dans le cas général la fonction dont le domaine de définition est composé de cortèges de longueur n est appelée *fonction de n variables*. Si f est une fonction de n variables au lieu de $f(\langle x_1, \ldots, x_n\rangle)$ on écrit $f(x_1, \ldots, x_n)$.

Composition des fonctions. Etudions les propriétés de la composition des fonctions. Sous composition des fonctions on comprend ici la composition des relations.

THÉORÈME 3.1. *Soient f et g des fonctions. Leur composition $f \circ g$ est alors également une fonction, telle que*

(1) $\text{Dom } f \circ g = \{x \mid g(x) \in \text{Dom } f\}$;

(2) $(f \circ g)(x) = f(g(x))$ *pour chaque* $x \in \text{Dom}(f \circ g)$;

(3) $f \circ g = \{\langle x, f(g(x))\rangle \mid g(x) \in \text{Dom } f\}$.

Démonstration. Par définition, la composition des relations binaires $f \circ g$ est un ensemble de tous les couples $\langle x, y\rangle$, tels que pour un certain z sont simultanément satisfaits $\langle x, z\rangle \in g$ et $\langle z, y\rangle \in f$, c'est-à-dire que

$$f \circ g = \{\langle x, y\rangle \mid \exists z (\langle x, z\rangle \in g \wedge \langle z, y\rangle \in f)\}.$$

Comme g est une fonction, $\langle x, z\rangle \in g$ signifie que $x \in \text{Dom } g$ et $z = g(x)$. Puisque f est une fonction, l'inclusion $\langle z, y\rangle \in f$ signifie que

$$z = g(x) \in \text{Dom } f \quad \text{et} \quad y = f(z) = f(g(x)).$$

Par conséquent,

$$f \circ g = \{\langle x, y\rangle \mid \langle g(x), y\rangle \in f\};$$
$$\langle x, y\rangle \in f \circ g \leftrightarrow y = f(g) \wedge (g(x) \in \text{Dom } f);$$
$$f \circ g = \{\langle x, f(g(x))\rangle \mid g(x) \in \text{Dom } f\}.$$

Donc, $f \circ g$ est une fonction qui satisfait les égalités (1), (2), (3). □

COROLLAIRE 3.2. *Soient f, g des fonctions quelconques; on a*

(a) $\text{Dom}(f \circ g) \subset \text{Dom } g$, $\text{Im}(f \circ g) \subset \text{Im } f$;

(b) *si* $\text{Im } g \subset \text{Dom } f$, *alors* $\text{Dom}(f \circ g) = \text{Dom } g$;

(c) *si* $\text{Im } g = \text{Dom } f$, *alors* $\text{Dom}(f \circ g) =$
$= \text{Dom } g$ et $\text{Im}(f \circ g) = \text{Im } f$.

THÉORÈME 3.3. *Si g est une application de l'ensemble A dans B et f une application de l'ensemble B dans C, alors $f \circ g$ est une application de l'ensemble A dans C.*

Démonstration. Par hypothèse, $\text{Im } g \subset \text{Dom } f = B$. Selon le corollaire 3.2, il s'ensuit que

$$\text{Dom } f \circ g = \text{Dom } g = A, \qquad \text{Im } f \circ g \subset \text{Im } f \subset C.$$

Par conséquent, $f \circ g$ est une application de l'ensemble A dans C. □

THÉORÈME 3.4. *Si g est une application de l'ensemble A sur B et f une application de l'ensemble B sur C, $f \circ g$ est alors une application de l'ensemble A sur C.*

Ce théorème découle directement du théorème 3.3 et du corollaire 3.2.

THÉORÈME 3.5. *La composition des fonctions est associative, c'est-à-dire* $f \circ (g \circ h) = (f \circ g) \circ h$ *pour toutes fonctions* f, g *et* h.

Le théorème 3.5 découle directement du théorème 2.2.

DÉFINITION. L'application i_A de l'ensemble A sur lui-même, telle que $i_A(x) = x$ pour chaque x de A est dite *application identique* (ou *unitaire*) *de l'ensemble* A *sur lui-même*.

THÉORÈME 3.6. *Soit* f *l'application de l'ensemble* A *sur* B. *Alors* $f \circ f^{\smile} = i_B$.

D é m o n s t r a t i o n. L'inversion $f^{\smile}$ de la fonction f est une relation binaire, telle que

$$f^{\smile} = \{\langle y, x\rangle \mid \langle x, y\rangle \in f\}.$$

Par définition de la composition des relations

(1) $$f \circ f^{\smile} = \{\langle y, z\rangle \mid \exists x\,(\langle y, x\rangle) \in f^{\smile} \wedge \langle x, z\rangle \in f\}.$$

De $\langle y, x\rangle \in f^{\smile}$ et $\langle x, z\rangle \in f$, il vient

(2) $$\langle x, y\rangle \in f \quad \text{et} \quad \langle x, z\rangle \in f.$$

Comme f est une fonction, de (2) s'ensuit l'égalité $y = z$. Donc (1) peut s'écrire sous la forme

$$f \circ f^{\smile} = \{\langle y, y\rangle \mid \exists x\,(\langle x, y\rangle \in f)\}.$$

D'où, puisque f est l'application de A sur B,

$$f \circ f^{\smile} = \{\langle y, y\rangle \mid y \in B\}.$$

Par conséquent, $f \circ f^{\smile} = i_B$. □

THÉORÈME 3.7. *Soient* f, g, h *les fonctions satisfaisant à la condition*

(1) $$\text{Dom}\, g = \text{Dom}\, h \subset \text{Im}\, f.$$

Alors, si $g \circ f = h \circ f$, *on a* $g = h$.

D é m o n s t r a t i o n. Supposons que

(2) $$g \circ f = h \circ f.$$

En vertu de (1) pour tout y de Dom g il se trouvera un élément x, tel que $y = f(x)$. D'où, en vertu de (2), il s'ensuit que

$$g(y) = g(f(x)) = h(f(x)) = h(y),$$

c'est-à-dire que $g(y) = h(y)$ pour tout y de Dom g. En outre, en vertu de (1) Dom g = Dom h. Donc $g = h$. □

Fonctions injectives. Parmi les fonctions étudiées en mathématiques un rôle important revient aux fonctions injectives.

DÉFINITION. La fonction f est dite *injective* si pour tous x, y (extraits de Dom f) il s'ensuit de la condition $f(x) = f(y)$ que $x = y$.

En d'autres termes, la fonction f est injective si pour tous x, y, z du fait que $\langle x, z\rangle \in f$ et $\langle y, z\rangle \in f$ il découle que $x = y$.

En vertu de la loi de contraposition il s'ensuit de la définition que *la fonction* f *est injective si et seulement si pour* x, y *quelconques*, la fonction f prend des valeurs différentes *au cas où* $x \neq y$, $f(x) \neq \neq f(y)$, autrement dit, pour des arguments différents.

Définition. Une application injective d'un ensemble non vide A sur lui-même est appelée *permutation de l'ensemble* A ou *transformation de l'ensemble* A.

En particulier, une application identique ou unitaire i_A de l'ensemble A sur lui-même est une permutation, c'est-à-dire une application telle que $i_A(x) = x$ pour chaque x de A.

Proposition 3.8. *Si* f *est une application de l'ensemble* A *dans l'ensemble* B, *on a* $f \circ i_A = f$, $i_B \circ f = f$. □

Théorème 3.9. *La composition de deux fonctions injectives quelconques est une fonction injective.*

Démonstration. Soient f et g des fonctions injectives. En vertu de l'application injective f pour tous x, y, si $f(g(x)) = = f(g(y))$, on a $g(x) = g(y)$. Ensuite, en vertu de l'application injective g pour tous x, y, quand $g(x) = g(y)$, on a $x = y$. Donc, pour x, y quelconques, si $f(g(x)) = f(g(y))$, on a $x = y$. Par conséquent, pour tous x, y quand $(f \circ g)(x) = (f \circ g)(y)$, on a $x = y$. La fonction $f \circ g$ est donc injective. □

Corollaire 3.10. *Une composition de deux permutations quelconques de l'ensemble* A *est une permutation de l'ensemble* A.

Ce corollaire découle directement des théorèmes 3.4 et 3.9.

Soit f une fonction. L'inversion $f^{\smile} = \{\langle x, y\rangle \mid \langle y, x\rangle \in f\}$ de la fonction f peut ne pas être une fonction. Ainsi, par exemple, si est donnée une fonction $f = \{\langle x, x^2\rangle \mid x \in \mathbf{Z}\}$, où $\mathbf{Z}$ est l'ensemble de tous les entiers, la relation $f^{\smile} = \{\langle x^2, x\rangle \mid x \in \mathbf{Z}\}$ n'est pas une fonction, car elle ne contient pas de couples $\langle 1, 1\rangle$ et $\langle 1, -1\rangle$ à éléments premiers identiques et éléments seconds différents.

Cependant pour une fonction $g = \{\langle x, 2x\rangle \mid x \in \mathbf{N}\}$, où $\mathbf{N}$ est l'ensemble de tous les entiers non négatifs, l'inversion $g^{\smile} = = \{\langle 2x, x\rangle \mid x \in \mathbf{N}\}$ est une fonction.

Proposition 3.11. *Si* f *et* g *sont des fonctions, on a*

(a) $\operatorname{Dom} f^{\smile} = \operatorname{Im} f$; (c) $(f^{\smile})^{\smile} = f$;

(b) $\operatorname{Im} f^{\smile} = \operatorname{Dom} f$; (d) $(f \circ g)^{\smile} = g^{\smile} \circ f^{\smile}$.

Cette proposition se déduit directement de la proposition 2.1 et du théorème 2.3.

Corollaire 3.12. *Si* f *est une application de l'ensemble* A *sur* B *et* $f^{\smile}$ *une fonction*, $f^{\smile}$ *est une application de l'ensemble* B *sur* A.

Théorème 3.13. *L'inversion* $f^{\smile}$ *de la fonction* f *est une fonction si et seulement si la fonction* f *est injective.*

Démonstration. La relation $f^{\smile}$ est une fonction si et seulement si pour tous x, y, z on a $x = y$ au cas où $\langle z, x\rangle \in f^{\smile}$ et

$\langle z, y \rangle \in f^{\smile}$. Cette condition est équivalente à la condition stipulant que la fonction f est injective:

pour tous x, y, z si $\langle x, z \rangle \in f$ et $\langle y, z \rangle \in f$, on a $x = y$. Par conséquent, la relation $f^{\smile}$ est une fonction si et seulement si la fonction f est injective. □

COROLLAIRE 3.14. *Si f est une fonction injective, $f^{\smile}$ l'est aussi. En outre, si f est une application injective de A sur B, $f^{\smile}$ est alors une application injective de B sur A.*

THÉORÈME 3.15. *Soient f, g, h des fonctions satisfaisant aux conditions:*

(1) $f \circ g = f \circ h$;

(2) $\text{Dom } g = \text{Dom } h, \quad \text{Im } g \subset \text{Dom } f, \quad \text{Im } h \subset \text{Dom } f.$

Dans ce cas si la fonction f est injective, on a $g = h$.

D é m o n s t r a t i o n. Supposons que la fonction f est injective. En vertu des conditions (1) et (2), on a

$$f(g(x)) = f(h(x)) \text{ pour tout } x \text{ de Dom } g.$$

En raison de l'application injective f on a $g(x) = h(x)$ pour tout x de Dom g. De plus, selon (2) Dom g = Dom h. Donc, $g = h$. □

Fonctions inversibles. Soit f l'application de l'ensemble A sur B.

DÉFINITION. La fonction φ est appelée *inverse à gauche* de la fonction f si φ est l'application de B sur A et si $\varphi \circ f = i_A$. La fonction possédant une inverse à gauche est dite *inversible à gauche.*

DÉFINITION. La fonction h est appelée *inverse à droite* de la fonction f si h est l'application de B sur A et si $f \circ h = i_B$. La fonction possédant une inverse à droite est dite *inversible à droite.*

DÉFINITION. La fonction g est dite *inverse* de la fonction f si g est l'application de B sur A, $g \circ f = i_A$ et $f \circ g = i_B$. La fonction possédant une inverse est dite *inversible.* La fonction inverse de la fonction f est désignée par le symbole f^{-1}.

Il découle de ces définitions: a) si φ est la fonction inverse à gauche de f, la fonction f est alors l'inverse à droite de φ; b) si h est la fonction inverse à droite de f, la fonction f est alors l'inverse à gauche de h; c) si la fonction g est l'inverse de f, la fonction f est alors l'inverse de g; dans ce cas les fonctions f et g sont dites *mutuellement inverses.*

THÉORÈME 3.16. *Si f est l'application injective de l'ensemble A sur B, on a alors $f^{\smile} \circ f = i_A$, $f \circ f^{\smile} = i_B$.*

D é m o n s t r a t i o n. Soit f l'application injective de l'ensemble A sur B. Alors, selon le théorème 3.13, la relation $f^{\smile}$ est aussi une fonction, pour tous x, y la condition

(1) $f^{\smile}(y) = x$

étant équivalente à

(2) $f(x) = y$.

En vertu de (2) et (1) pour tout x de A, il vient

$$f^{\smile}(f(x)) = x \quad \text{et} \quad (f^{\smile} \circ f)(x) = x,$$

soit $f^{\smile} \circ f = i_A$. Ensuite, en vertu de (1) et (2) pour tout y de B, on a

$$f(f^{\smile}(y)) = y \quad \text{et} \quad (f \circ f^{\smile})(y) = y,$$

soit $f \circ f^{\smile} = i_B$. □

COROLLAIRE 3.17. *Si f est une application injective de l'ensemble A sur B, f est une fonction inversible, la fonction $f^{\smile}$ est l'inverse de f.*

COROLLAIRE 3.18. *Si f est une permutation de l'ensemble A, $f^{\smile} \circ f = i_A$ et $f \circ f^{\smile} = i_A$.*

THÉORÈME 3.19. *Soit f une application de l'ensemble A sur B inversible à gauche. Toute fonction inverse à gauche de f coïncide avec $f^{\smile}$ et est également une inverse à droite de f qui est inversible.*

Démonstration. Soit $\varphi: B \to A$ est une fonction inverse à gauche de f, c'est-à-dire

(1) $\varphi \circ f = i_A$.

Suivant le théorème 3.6 et la proposition 3.8, il vient

(2) $f \circ f^{\smile} = i_B, \qquad i_A \circ f^{\smile} = f^{\smile}, \qquad \varphi \circ i_B = \varphi$.

En vertu de (2) et (1),

$$\varphi = \varphi \circ i_B = \varphi \circ (f \circ f^{\smile}) = (\varphi \circ f) \circ f^{\smile} = i_A \circ f^{\smile} = f^{\smile},$$

donc, $\varphi = f^{\smile}$. En outre, $f \circ \varphi = f \circ f^{\smile} = i_B$, la fonction φ est également une inverse à droite de f et, par suite, f est inversible. □

THÉORÈME 3.20. *Soit f l'application de l'ensemble A sur B inversible à droite. Toute fonction inverse à droite de f coïncide avec $f^{\smile}$ et est également une inverse à gauche de f qui est inversible.*

Démonstration. Soit $h: B \to A$ est la fonction inverse à droite de f, c'est-à-dire

(1) $f \circ h = i_B$.

Suivant le théorème 3.6 et la proposition 3.8, on a

(2) $h \circ h^{\smile} = i_A, \qquad i_B \circ h^{\smile} = h^{\smile}$.

En vertu de (2) et (1), il vient

$$f = f \circ i_A = f \circ (h \circ h^{\smile}) = (f \circ h) \circ h^{\smile} = i_B \circ h^{\smile} = h^{\smile}.$$

Selon le théorème 2.1 de $f = h^{\smile}$ s'ensuit $h = f^{\smile}$. De plus, $h \circ f = f^{\smile} \circ f = i_A$, c'est-à-dire que la fonction h est également une inverse à gauche de f et, partant, f est inversible. □

THÉORÈME 3.21. *Les propriétés suivantes de la fonction f sont équipotentes*:

(a) *l'inversion $f^{\smile}$ de la fonction f est une fonction*;
(b) *la fonction f est injective*;
(c) *la fonction f est inversible à droite*;
(d) *la fonction f est inversible à gauche*;
(e) *la fonction f est inversible*;
(g) *toutes les fonctions inverses de f (à gauche, à droite, bilatères) existent et coïncident avec $f^{\smile}$.*

D é m o n s t r a t i o n. Selon le théorème 3.13, les propriétés (a) et (b) sont équipotentes.

Si f est une application injective de A sur B, alors selon le théorème 3.14 $f^{\smile}$ est une application de B sur A et $f \circ f^{\smile} = i_B$, la fonction f est inversible à droite. Par conséquent, de (b) se déduit (c).

Si la fonction f est inversible à droite, alors, selon le théorème 3.20, elle est également inversible à gauche. Donc, de (c) s'ensuit (d). Si la fonction f est inversible à gauche, alors en vertu du théorème 3.19, la fonction f est inversible. Par conséquent, de (d) découle (e).

Supposons que la fonction f est inversible. Elle est alors inversible à gauche et à droite. Selon les théorèmes 3.19 et 3.20, toutes les fonctions inverses de f coïncident avec $f^{\smile}$.

Si la condition (g) est satisfaite, l'inversion $f^{\smile}$ de la fonction f est une fonction. Donc, de (g) s'ensuit (a).

Par conséquent, les propriétés (a), (b), (c), (d), (e), (g) sont équipotentes. □

THÉORÈME 3.22. *Si les fonctions f et g sont inversibles, la fonction $f \circ g$ l'est également et $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.*

D é m o n s t r a t i o n. Soient f et g des fonctions inversibles. Leurs inverses $f^{\smile}$ et $g^{\smile}$ sont alors des fonctions et

(1) $f^{\smile} = f^{-1}, \qquad g^{\smile} = g^{-1}.$

Selon le théorème 2.3, il vient

(2) $(f \circ g)^{\smile} = g^{\smile} \circ f^{\smile}.$

Comme $g^{\smile}$ et $f^{\smile}$ sont des fonctions, leur composition $g^{\smile} \circ f^{\smile}$ est une fonction; donc, en vertu de (2), $(f \circ g)^{\smile}$ est une fonction. Aussi la fonction $f \circ g$ est-elle inversible et on a:

(3) $(f \circ g)^{\smile} = (f \circ g)^{-1}.$

Sur la base des égalités (1), (2), (3) on conclut que la fonction $f \circ g$ est inversible et $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$. □

Restriction d'une fonction. Un cas particulier de restriction d'une relation binaire est la restriction d'une fonction.

DÉFINITION. La fonction g est dite *restriction* (ou *striction*) *de la fonction* f si $g \subset f$. Si $g \subset f$ on dit également que f est l'*extension* (ou *prolongement*) *de la fonction* g.

DÉFINITION. La fonction g est appelée *restriction de la fonction* f *par l'ensemble* A (ou *striction de la fonction* f *à l'ensemble* A) si $g \subset f$ et $\mathrm{Dom}\, g = A$.

La restriction de la fonction f à l'ensemble A est notée f_A ou $f \mid A$.

PROPOSITION 3.23. *Si* $A \subset \mathrm{Dom}\, f$, *la fonction* $f \circ i_A$ *est alors une restriction de la fonction* f *à l'ensemble* A, c'est-à-dire $f_A = f \circ i_A$.

Cette proposition découle directement de la définition de la fonction f_A.

THÉORÈME 3.24. *La fonction* g *est une restriction de la fonction* f *si et seulement si* $\mathrm{Dom}\, g \subset \mathrm{Dom}\, f$ *et* $g(x) = f(x)$ *pour tout* x *extrait de* $\mathrm{Dom}\, g$.

Démonstration. Supposons que $g \subset f$. Alors, $\mathrm{Dom}\, g \subset \subset \mathrm{Dom}\, f$ et pour tout $x \in \mathrm{Dom}\, g$ de $\langle x, y \rangle \in g$ s'ensuit $\langle x, y \rangle \in f$, et, par conséquent, $g(x) = f(x)$.

Admettons maintenant que $\mathrm{Dom}\, g \subset \mathrm{Dom}\, f$ et $g(x) = f(x)$ pour tout $x \in \mathrm{Dom}\, g$. Alors, pour tous x, y de $\langle x, y \rangle \in g$, c'est-à-dire de $y = g(x)$, il s'ensuit que $y = f(x)$ et $\langle x, y \rangle \in f$, donc, $g \subset f$. □

Exercices

1. Parmi les relations suivantes lesquelles sont des fonctions? Indiquer leurs domaines de définition et leurs domaines des valeurs:

(a) $\{\langle x, y \rangle \mid x, y \in \mathbf{N}$ et $y = x^2\}$;

(b) $\{\langle x, y \rangle \mid x, y \in \mathbf{N}$ et $x < y \leqslant x + 1\}$;

(c) $\{\langle x, y \rangle \mid x, y \in \mathbf{Z}$ et $y = x^2\}$;

(d) $\{\langle x, y \rangle \mid x, y \in \mathbf{N}$ et x divise $y\}$;

(e) $\{\langle x, y \rangle \mid x, y \in \mathbf{Z}$ et $y = \mid x \mid\}$;

(f) $\{\langle x, y \rangle \mid x, y \in \mathbf{Z}$ et $x = y^2\}$.

Ici et plus loin $\mathbf{Z}$ est l'ensemble de tous les entiers, $\mathbf{N}$ l'ensemble de tous les entiers non négatifs.

2. Soit $A = \{0, 1\}$ un ensemble à deux éléments. Rechercher toutes les applications de l'ensemble A sur lui-même et indiquer celles qui sont injectives.

3. Rechercher toutes les applications de l'ensemble $A = \{0, 1, 2\}$ sur l'ensemble $B = \{0, 1\}$.

4. Démontrer que pour chaque fonction f et un ensemble quelconque A $f(A) = \varnothing$ si et seulement si $A \cap \mathrm{Dom}\, f = \varnothing$.

5. Démontrer que si f est une application de l'ensemble A sur A telle que $f \circ f = f$, on a $f = i_A$.

6. Démontrer que si f est une fonction et A et B des ensembles, alors $f(A \cap B) \subset f(A) \cap f(B)$. Montrer à l'aide d'exemples que l'égalité $f(A \cap B) = = f(A) \cap f(B)$ peut ne pas avoir lieu.

7. Soit $R \subset A \times B$. Démontrer que R est l'application de l'ensemble A dans B si et seulement si $R \circ R^{\smile} \subset i_B$ et $i_A \subset R^{\smile} \circ R$.

8. Démontrer que chacune des fonctions suivantes possède une inverse. Chercher le domaine de définition de la fonction inverse:

(a) $f = \{\langle x, y\rangle \mid x, y \in \mathbf{N} \text{ et } y = 2x + 1\}$;

(b) $f = \{\langle n, n^2\rangle \mid n \in \mathbf{N}\}$;

(c) $f = \{\langle x, y\rangle \mid x, y \in \mathbf{N} \text{ et } y = x^3\}$.

9. Pour tous ensembles A, B et C démontrer qu'il existe:

(a) une application injective de l'ensemble $A \times B$ sur $B \times A$;

(b) une application injective de l'ensemble $(A \times B) \times C$ sur $A \times (B \times C)$.

10. Soit f une application de l'ensemble A dans A. Démontrer que si $f \circ f \circ f = i_A$, f est une application injective de l'ensemble A sur A.

11. Soit f une application de l'ensemble A dans B. Montrer que si $C, D \subset B$ et $C \cap D = \varnothing$, alors $f^{\smile}(A) \cap f^{\smile}(B) = \varnothing$.

12. Démontrer que pour toute fonction f sont satisfaites les relations:

(a) $f^{\smile}(A \cup B) = f^{\smile}(A) \cup f^{\smile}(B)$;

(b) $f^{\smile}(A \cap B) = f^{\smile}(A) \cap f^{\smile}(B)$;

(c) $f^{\smile}(A \setminus B) = f^{\smile}(A) \setminus f^{\smile}(B)$;

(d) $A \subset B \rightarrow f^{\smile}(A) \subset f^{\smile}(B)$.

13. Démontrer que si $A \subset \operatorname{Dom} f$ et $B \subset \operatorname{Im} f$, on a alors

(a) $A \subset f^{\smile}(f(A))$; (b) $f(f^{\smile}(B)) = B$.

14. Démontrer que $f(A) \setminus f(B) \subset f(A \setminus B)$ pour chaque fonction f et tous ensembles A et B. Si f est une fonction injective, on a $f(A) \setminus f(B) = f(A \setminus B)$ pour tous ensembles A et B.

15. Soient f une application de l'ensemble A dans B et g une application de l'ensemble B dans C. Démontrer que:

(a) si l'application $g \circ f$ est injective, f l'est également; (b) si $g \circ f$ est une application de A sur C, g est une application de B sur C.

16. Démontrer que l'application $f: A \rightarrow B$ est une application injective de l'ensemble A sur B si et seulement s'il existe une application $g: B \rightarrow A$ telle que $g \circ f = i_A$ et $f \circ g = i_B$.

17. Démontrer que la relation binaire $R \subset A \times B$ est une application injective de l'ensemble A sur B si et seulement si $R \circ R^{\smile} = i_B$ et $R^{\smile} \circ R = i_A$.

18. Démontrer que la fonction f satisfait à la condition $f(A \cap B) = f(A) \cap f(B)$ pour tous ensembles A et B si et seulement si la fonction f est injective.

19. Soient A et B des ensembles finis composés de m et n éléments respectivement, avec $m \leqslant n$. Démontrer qu'il existe $n(n-1)\ldots(n-m+1)$ applications injectives de l'ensemble A dans B.

20. Soient A et B des ensembles finis composés de m et n éléments respectivement.

(a) pour quels m et n existe-t-il des applications injectives de l'ensemble A dans B?

(b) Combien y a-t-il d'applications de l'ensemble A dans B?

(c) Combien a-t-on de relations binaires entre les éléments des ensembles A et B?

§ 4. Relation d'équivalence

Quelques types de relations binaires. D'après certaines propriétés importantes on divise les relations binaires en types.

DÉFINITION. La relation binaire R sur l'ensemble A est *réflexive* sur A si pour chaque x de A, on a xRx.

La relation R est réflexive sur A si et seulement si $i_A \subset R$, où $i_A = \{\langle x, x\rangle \mid x \in A\}$. Si la relation R est réflexive, alors chaque sommet de son graphe est en lacet. Inversement : un graphe dont chaque sommet a un lacet représente une certaine relation réflexive.

En guise d'exemples de relations réflexives on peut indiquer la relation de parallélisme sur un ensemble de droites du plan, la relation d'égalité sur un ensemble quelconque de nombres et la relation de divisibilité sur un ensemble quelconque d'entiers.

DÉFINITION. La relation binaire R sur l'ensemble A est *antiréflexive* sur A si pour chaque x de A $\langle x, x\rangle \notin R$, c'est-à-dire si pour chaque x de A la condition xRx n'est pas remplie.

La relation R est antiréflexive sur A si et seulement si $i_A \cap R = \varnothing$. Si la relation R est antiréflexive, aucun sommet de son graphe n'est en lacet. Réciproquement : si aucun sommet du graphe ne comporte de lacet, le graphe représente une relation antiréflexive.

Par exemple, la relation d'inégalité ($\neq$) sur un ensemble quelconque de nombres et la relation de perpendicularité sur un ensemble de droites du plan sont antiréflexives.

DÉFINITION. La relation binaire R (sur A) est dite *transitive* (sur A) si pour tous x, y, z du domaine de la relation R (sur A) de xRy et yRz s'ensuit xRz.

La relation R est transitive si et seulement si $R \circ R \subset R$. Si la relation R est transitive, son graphe, pour chaque couple d'arêtes $\langle x, y\rangle$ et $\langle y, z\rangle$, possède une arête de fermeture $\langle x, z\rangle$ et réciproquement.

Par exemple, la relation de divisibilité sur un ensemble d'entiers est transitive. La relation d'inégalité ($\neq$) n'est pas transitive.

DÉFINITION. Une relation binaire R (sur A) est dite *symétrique* (sur A) si pour des x, y quelconques du domaine de la relation R (de A) de xRy s'ensuit yRx.

La relation R est symétrique si et seulement si $R^{\smile} = R$. Si la relation R est symétrique, chaque arête de son graphe n'est pas orientée. Réciproquement : un graphe aux arêtes non orientées représente une certaine relation binaire symétrique.

Par exemple, sont symétriques les relations de parallélisme de droites, la relation de perpendicularité de droites et la relation d'égalité.

DÉFINITION. Une relation binaire R (sur A) est dite *antisymétrique* (sur A) si pour des x, y quelconques du domaine de la relation R (de A) de xRy et yRx s'ensuit $x = y$.

La relation R est antisymétrique sur A si et seulement si $R \cap R^{\smile} \subset i_A$. Le graphe de la relation antisymétrique n'a pas d'arêtes non orientées, mais peut posséder des lacets.

Par exemple, la relation d'inclusion $\subset$ sur une collection quelconque d'ensembles est antisymétrique.

DÉFINITION. Une relation binaire R sur un ensemble A est dite

liée sur A si pour tous éléments x, y de l'ensemble A de $x \neq y$ s'ensuit $xRy \vee yRx$.

Une relation R est liée sur A si et seulement si $A \times A \setminus i_A \subset \subset R \cup R^{\smile}$.

Une relation binaire R sur A est liée sur A si et seulement si pour tous x, y de A on a *soit* $x = y$, *soit* xRy, *soit* yRx, c'est-à-dire $A \times A = i_A \cup R \cup R^{\smile}$.

Le graphe d'une relation liée est doué des propriétés suivantes: deux sommets quelconques (différents) du graphe sont réunis par une arête. La réciproque est également vraie.

C'est ainsi par exemple, que la relation banale « inférieur à » ($<$) sur une collection quelconque de nombres est une relation liée.

Relation d'équivalence. Une relation binaire importante est la relation d'équivalence.

DÉFINITION. La relation binaire sur l'ensemble A est appelée *relation d'équivalence* sur A si elle est réflexive, symétrique et transitive (sur A).

La relation d'équivalence est souvent désignée par les symboles $\sim$, $\approx$ ou $\equiv$.

E x e m p l e s. 1. Soient A un ensemble non vide et $i_A = \{\langle x, x\rangle \mid x \in A\}$ une relation d'identité sur l'ensemble A. La relation i_A est la relation d'équivalence sur A.

2. Soient A un ensemble de droites du plan et

$$R = \{\langle x, y\rangle \mid x, y \in A \quad \text{et} \quad x \text{ est parallèle à } y\}$$

la relation de parallélisme. La relation de parallélisme sur A est une relation d'équivalence.

3. Soient $\mathbf{Z}$ l'ensemble de tous les entiers et m un nombre entier différent de zéro. La relation

$$R = \{\langle x, y\rangle \mid x, y \in \mathbf{Z} \quad \text{et} \quad x - y \text{ est divisible par } m\}$$

s'appelle *congruence modulo m*. Cette relation est une relation d'équivalence sur $\mathbf{Z}$.

4. Soit A un ensemble de segments orientés d'un plan donné. La relation d'équipollence des segments orientés est une relation d'équivalence sur A.

5. La relation de similitude sur un ensemble de triangles d'un plan donné est une relation d'équivalence.

6. Deux ensembles sont dits *équipotents* s'il existe une application injective d'un ensemble sur l'autre. La relation d'équipotence sur une collection donnée quelconque d'ensembles est une relation d'équivalence.

DÉFINITION. Soient R une relation d'équivalence sur A et $a \in A$. On appelle *classe d'équivalence engendrée par l'élément a* l'ensemble $\{x \in A \mid xRa\}$, c'est-à-dire un ensemble de tels x de A pour lesquels $\langle x, a\rangle \in R$.

La classe d'équivalence engendrée par l'élément a est notée a/R ou $[a]_R$. La collection de toutes les classes d'équivalence de la relation R sur l'ensemble A est notée A/R ou $[A]_R$.

DÉFINITION. Tout élément de la classe d'équivalence est dit représentant de cette classe. On appelle *système complet de représentants des classes d'équivalence* l'ensemble des représentants de toutes les classes, un par classe.

Dans l'exemple 1 les classes d'équivalence sont constituées par des sous-ensembles A à un élément. Dans l'exemple 2 les classes d'équivalence portent le nom de *faisceaux de droites parallèles*. Dans l'exemple 3 les classes d'équivalence s'appellent *classes résiduelles modulo m*, chaque classe étant composée de tous les nombres qui après division par m fournissent un même résidu. Dans l'exemple 4 les classes d'équivalence sont constituées par des *vecteurs* du plan. Dans l'exemple 5 les classes d'équivalence sont des ensembles de triangles semblables deux à deux. Dans l'exemple 6 les classes d'équivalence sont des classes d'ensembles équipotents.

Ensemble quotient. Soit A un ensemble non vide.

DÉFINITION. On appelle *ensemble quotient de l'ensemble A par l'équivalence R* l'ensemble A/R de toutes les classes d'équivalence.

DÉFINITION. On appelle *partition d'un ensemble A* une telle famille de ses sous-ensembles non vides pour laquelle chaque élément de A est strictement inclus dans un terme de la famille.

Autrement dit, la partition de l'ensemble A est une famille de ses sous-ensembles non vides dont la réunion coïncide avec A, tandis que l'intersection de deux quelconques de ces sous-ensembles est vide.

THÉORÈME 4.1. *Soit R une relation d'équivalence sur un ensemble A (non vide). Alors l'ensemble quotient A/R est une partition de l'ensemble A.*

D é m o n s t r a t i o n. Chaque élément a de l'ensemble A appartient à la classe d'équivalence a/R. Il faut démontrer que chaque élément de A appartient strictement à un terme de la famille A/R. Pour cela il suffit de montrer que les classes d'équivalence possédant au moins un élément commun coïncident. Soient a/R et b/R les classes d'équivalence à élément commun c, x étant un élément quelconque de a/R, on a alors xRa, aRc, cRb et en vertu de la transitivité de la relation R xRb. Ainsi, $a/R \subset b/R$. De façon analogue on démontre que $b/R \subset a/R$. On a donc $a/R = b/R$. Bref, on a établi que l'ensemble quotient A/R est une partition de l'ensemble A. □

COROLLAIRE 4.2. *Soit R une relation d'équivalence sur l'ensemble A, alors*

(1) $a \in a/R$ *pour tout* a *de* A ;

(2) *pour tous* a, b *de* A $a/R = b/R$ *si et seulement si* aRb ;

(3) $a/R \neq b/R$ *si et seulement si* $a/R \cap b/R = \varnothing$;

(4) $A = \bigcup_{x \in A} x/R$.

Ce corollaire découle directement du théorème 4.1.

Soient S une partition de l'ensemble non vide A et R_S une relation binaire définie de la façon suivante: $\langle x, y\rangle \in R_S$ si et seulement si x et y appartiennent au même terme de la famille S.

THÉORÈME 4.3. *La relation R_S associée à la partition S d'un ensemble non vide A est une relation d'équivalence sur A, en outre, l'ensemble quotient A/R_S coïncide avec la partition S.*

La démonstration du théorème s'effectue sans peine et on laisse au lecteur le soin de l'esquisser en guise d'exercice.

Équivalence d'application. Soit f l'application de l'ensemble A dans B. Considérons une relation binaire R sur A telle que xRy n'ait lieu que si et seulement si $f(x) = f(y)$.

DÉFINITION. Soit f une application de l'ensemble A dans B. La relation binaire R,

$$R = \{\langle x, y\rangle \mid f(x) = f(y), \quad x, y \in A\},$$

est appelée *équivalence d'application* f.

THÉORÈME 4.4. *Soient f une application quelconque et A = Dom f. La relation d'équivalence d'application f est une relation d'équivalence sur l'ensemble A.*

Démonstration. Soit R une équivalence d'application f. La relation R est réflexive sur A, car $f(x) = f(x)$ pour tout x de A. La relation R est transitive, car pour tous x, y, z il s'ensuit de $f(x) = f(y)$ et $f(y) = f(z)$ que $f(x) = f(z)$. La relation R est symétrique, car pour tous x, y de $f(x) = f(y)$ s'ensuit $f(y) = f(x)$. Par conséquent, R est une relation d'équivalence sur l'ensemble A. □

Si $a \in A = \text{Dom } f$, $f(a) = b$ et R est une équivalence d'application f, la classe d'équivalence engendrée par l'élément a est $f^{\smile}(b)$. L'ensemble $\{f^{\smile}(x) \mid x \in \text{Im } f\}$ est l'ensemble quotient de l'ensemble A relativement à l'équivalence R, c'est-à-dire $A/R = \{f^{\smile}(x) \mid x \in \text{Im } f\}$.

Toute relation d'équivalence R_1 sur un ensemble A peut être assimilée à une relation d'équivalence d'une certaine application de l'ensemble A. En effet, on peut définir l'*application naturelle de l'ensemble A sur l'ensemble quotient A/R_1* en associant à chaque x de A la classe d'équivalence unique x/R_1 contenant x. On vérifie sans peine que la relation d'équivalence R_1 coïncide avec l'équivalence d'application naturelle de l'ensemble A sur A/R_1.

Exercices

1. Etudier les relations suivantes sous l'angle de la réflexivité, de la nonréflexivité, de la symétrie, de l'antisymétrie, de la transitivité:

(a) $\{\langle x, y\rangle \mid x, y \in \mathbf{Z}$ et $x \leqslant y + 1\}$, où $\mathbf{Z}$ est l'ensemble de tous les entiers;

(b) $\{\langle x, y\rangle \mid x, y \in \mathbf{Z}$ et $x^2 = y^2\}$;
(c) $\{\langle x, y\rangle \mid x, y \in \mathbf{Z}$ et $|x| = |y|\}$;
(d) $\{X, Y \mid X, Y \subset \mathbf{Z}$ et $X \cap Y = \varnothing\}$;
(e) $\{\langle x, y\rangle \mid x, y \in \mathbf{N}$ et x divise $y\}$ (N est l'ensemble de tous les entiers non négatifs);
(f) $\{\langle x, y\rangle \mid x, y \in \mathbf{N}$ et $x < y\}$;
(g) $\{\langle x, y\rangle \mid x, y \in \mathbf{N}$ et $x + y = 1\}$;
(h) $\{\langle x, y\rangle \mid x, y \in \mathbf{N}$ et $x \leqslant y\}$;
(i) $\{\langle x, y\rangle \mid x, y \in \mathbf{N}$ et $x \neq y\}$;
(j) $\{\langle x, y\rangle \mid x, y \in \mathbf{Z}$ et $x^2 + x = y^2 + y\}$;
(k) $\{\langle x, y\rangle \mid x, y \in \mathbf{Z}$ et $x^2 + y^2 = 1\}$.

2. Donner des exemples de relations binaires:
(a) réflexives et transitives mais non pas antisymétriques;
(b) transitives et symétriques mais non pas réflexives;
(c) réflexives et transitives mais non pas symétriques;
(d) réflexives et symétriques mais non pas transitives.

3. Soit $R \subset A \times A$. Démontrer que:
(a) R est réflexif sur l'ensemble A si et seulement si $i_A \subset R$;
(b) R est symétrique si et seulement si $R^{\smile} \subset R$;
(c) R est transitif si et seulement si $R \circ R \subset R$.

4. Démontrer qu'une relation binaire R symétrique et antisymétrique est transitive.

5. Trouver tous les ensembles quotients de l'ensemble $\{1, 2, 3\}$.

6. Montrer que l'ensemble $\{1, 2, 3, 4\}$ possède 15 ensembles quotients différents.

7. Démontrer que si R est une relation binaire transitive et symétrique sur l'ensemble A, où A est le domaine de la relation R, R est une équivalence sur A.

8. Démontrer que la relation binaire R, dont le domaine de définition en Dom $R = A$, est une relation d'équivalence sur A si et seulement si $R \circ R \subset R$ et $R^{\smile} = R$.

9. Démontrer que si R est une relation d'équivalence sur l'ensemble A, $R^{\smile}$ est aussi une relation d'équivalence sur A.

10. Démontrer qu'une intersection de toute collection de relations d'équivalence sur l'ensemble A est une relation d'équivalence sur l'ensemble A.

11. Démontrer que pour tout ensemble M non vide il existe une application injective de l'ensemble de toutes les partitions de l'ensemble M sur l'ensemble de toutes les relations d'équivalence sur M.

12. Démontrer que l'ensemble quotient Z/mod m de l'ensemble des entiers Z suivant la congruence modulo m comporte exactement m éléments.

§ 5. Relations d'ordre

Relations d'ordre. Soit R une relation binaire sur l'ensemble A.

Définition. Une relation binaire R sur l'ensemble A est appelée *relation d'ordre sur A* ou *ordre sur A*, si elle est transitive et antisymétrique.

Définition. Une relation d'ordre R sur l'ensemble A est dite *non stricte* si elle est réflexive sur A, c'est-à-dire si $\langle x, x\rangle \in R$ pour tout x de A.

La relation d'ordre R est dite *stricte* (sur A) si elle est antiréflexive sur A, c'est-à-dire si $\langle x, x\rangle \notin R$ pour tout x de A. Or, comme la relation transitive R est antiréflexive elle est également antisymétrique. Aussi peut-on avancer la définition équivalente suivante.

DEFINITION. Une relation binaire R sur l'ensemble A est appelée *ordre strict sur A* si elle est transitive et n'est pas réflexive sur A.

Exemples. 1. Soit $P(M)$ l'ensemble de tous les sous-ensembles de l'ensemble M. La relation d'inclusion $\subset$ sur l'ensemble $P(M)$ est une relation d'ordre non strict.

2. Les relations $<$ et $\leqslant$ sur l'ensemble des nombres réels sont respectivement des relations d'ordre strict et non strict.

3. La relation de divisibilité dans un ensemble de nombres naturels est une relation d'ordre non strict.

DEFINITION. Une relation binaire R sur un ensemble A est appelée *relation de préordre* ou *préordre sur A* si elle est réflexive sur A et transitive.

Exemples. 1. La relation de divisibilité dans un ensemble de nombres entiers n'est pas un ordre. Or, elle est réflexive et transitive, c'est donc un préordre.

2. La relation $\models$ de déduction logique est une relation de préordre sur un ensemble des formules de la logique des assertions.

Ordre total. Un cas particulier important de la relation d'ordre est l'ordre total.

DEFINITION. Une relation d'ordre sur un ensemble A est appelée *relation d'ordre total sur A* si elle est liée sur A, c'est-à-dire si pour tous x, y de A on a

$$\text{soit } xRy, \text{ soit } x = y, \text{ soit } yRx.$$

Une relation d'ordre non total est habituellement appelée *relation d'ordre partiel* ou *ordre partiel*.

Exemples. 1. La relation « inférieur à » sur un ensemble de nombres réels est une relation d'ordre total.

2. La relation d'ordre adoptée dans les dictionnaires de la langue russe est dite *lexicographique*. L'ordre lexicographique sur l'ensemble des mots de la langue russe est un ordre total.

3. La relation d'inclusion $\subset$ sur la collection des sous-ensembles d'un ensemble donné M est une relation d'ordre partiel si M comporte au moins deux éléments différents.

Un même ensemble peut être totalement ordonné par des relations d'ordre différentes. C'est ainsi, par exemple, que sur un ensemble fini M non vide composé de n éléments on peut appliquer $n!$ ordres totaux différents.

Ensemble ordonné. Soit R une relation d'ordre quelconque sur un ensemble A non vide.

DEFINITION. On appelle *ensemble ordonné* le couple $\langle A, R\rangle$, où A est un ensemble non vide et R une relation d'ordre sur A. Si

l'ordre R sur A est total, le couple $\langle A, R\rangle$ est appelé *ensemble totalement ordonné*. Si l'ordre R sur A est partiel, alors le couple $\langle A, R\rangle$ est appelé *ensemble partiellement ordonné*.

DEFINITION. Soit $\langle A, \prec\rangle$ un ensemble ordonné. L'élément a de A est appelé *le plus petit* (*le plus grand*) *élément de* A si $a \prec x$ ($x \prec a$) pour tout élément x de A différent de a.

Tout ensemble ordonné ne comporte pas plus d'un plus petit élément et d'un plus grand élément.

DEFINITION. Soit $\langle A, \prec\rangle$ un ensemble ordonné. L'élément a est dit *minimal* (*maximal*) dans A au cas où est satisfaite la condition: pour tout x de A si $x \prec a$, $x = a$ (si $a \prec x$, alors $a = x$).

Un ensemble ordonné peut comporter plusieurs éléments minimaux et maximaux.

Exemple. Soit R la relation de divisibilité dans l'ensemble $\mathbf{N}\setminus\{0, 1\}$ ($\mathbf{N}$ est l'ensemble des nombres naturels). Dans l'ensemble ordonné $\langle \mathbf{N}\setminus\{0, 1\}, R\rangle$ tout nombre premier est un élément minimal.

Dans un ensemble totalement ordonné les notions d'éléments le plus petit (le plus grand) et minimal (maximal) coïncident.

DEFINITION. Un ensemble ordonné $\langle A, R\rangle$ est appelé *ensemble bien ordonné* si chaque sous-ensemble non vide de l'ensemble A possède le plus petit élément.

Exemples. 1. Si $<$ est la relation banale « inférieur à » sur l'ensemble $\mathbf{N}$ des nombres naturels, alors $\langle \mathbf{N}, <\rangle$ est un ensemble bien ordonné.

2. Soit $<$ la relation banale « inférieur à » sur l'ensemble $\mathbf{R}$ de tous les nombres réels. Dans ce cas l'ensemble totalement ordonné $\langle \mathbf{R}, <\rangle$ n'est pas un ensemble bien ordonné.

Exercices

1. Démontrer que l'application identique i_A de l'ensemble A est une relation d'ordre sur l'ensemble A.

2. Montrer que la relation

$$R = \{\langle x, y\rangle \mid x, y \in \mathbf{N} \quad (x \text{ divise } y \quad \text{ou} \quad x < y)\}$$

est un ordre total sur l'ensemble $\mathbf{N}$ des nombres naturels.

3. Soient $A = \{1, 2, 3, 4, 5, 6, 7\}$ et

$$R = \{\langle x, y\rangle \mid x, y \in A \quad \text{et} \quad (x - y) \vdots 2\}.$$

Montrer que R est une relation d'équivalence sur A.

4. Soient les relations $<$ et $\leqslant$ définies sur l'ensemble $\mathbf{N}$ des nombres naturels de façon banale. Démontrer que $< \circ < \neq <$; $\leqslant \circ < = <$; $\leqslant \circ \geqslant = \mathbf{N} \times \mathbf{N}$.

5. Construire un ordre total sur l'ensemble $\mathbf{N} \times \mathbf{N}$.

6. Montrer qu'un ensemble fini comportant n éléments peut être totalement ordonné par $n!$ procédés.

7. Montrer que la relation d'inclusion $\subset$ ne constitue pas un ordre total sur la collection $P(A)$ de tous les sous-ensembles de l'ensemble A, si A contient au moins deux éléments.

8. Démontrer que tout ensemble bien ordonné est un ensemble totalement ordonné.

9. Démontrer que la relation binaire R sur un ensemble A est une relation d'ordre non strict si et seulement si $R \circ R = R$ et $R \circ R^{\smile} = i_A$.

10. Démontrer que si R est une relation d'ordre (d'ordre total) la relation inverse $R^{\smile}$ est également une relation d'ordre (d'ordre total).

11. Soit $\leqslant$ une relation d'ordre non strict sur l'ensemble A. Démontrer que la relation $<$ n'est pas réflexive et est transitive sur A.

12. Soit $<$ une relation binaire non réflexive et transitive sur l'ensemble A. Démontrer que la relation $\leqslant$ est telle que $x \leqslant y \equiv (x < y) \vee (x = y)$ est une relation d'ordre non strict sur A.

13. Démontrer que pour un ensemble totalement ordonné les notions de *le plus grand* (*le plus petit*) et de *maximal* (de *minimal*) éléments coïncident.

14. Démontrer que si R est un ordre partiel (ordre total, bon ordre), sur l'ensemble A et $B \subset A$, $R \cap (B \times B)$ est un ordre partiel (total, bon) sur l'ensemble B.

15. Soit R la relation de préordre sur l'ensemble A. Posons $a \sim b \equiv (\langle a, b\rangle \in R \wedge \langle b, a\rangle \in R)$. Démontrer que:

(a) si $a \sim c$, $b \sim d$, $\langle a, b\rangle \in R$, alors $\langle c, d\rangle \in R$;

(b) $\sim$ est la relation d'équivalence sur A;

(c) R_1 est la relation d'ordre sur $A/\sim$, où $R_1 = \{\langle a/\sim, b/\sim\rangle \mid \langle a, b\rangle \in R\}$.

CHAPITRE III

ALGÈBRES ET SYSTÈMES ALGÉBRIQUES

§ 1. Opérations binaires

Opérations binaires et n-aires. Soit A un ensemble non vide.

DÉFINITION. *On appelle opération binaire sur l'ensemble A l'application de l'ensemble $A \times A$ dans A.*

L'addition et la multiplication banales des nombres entiers sont des exemples d'opérations binaires sur un ensemble d'entiers. Soit $P(M)$ l'ensemble de tous les sous-ensembles de l'ensemble M; la réunion $\cup$ et l'intersection $\cap$ sont des exemples d'opérations binaires sur l'ensemble $P(M)$.

Soit f une opération binaire quelconque sur l'ensemble A. Si dans l'application f l'élément c correspond au couple $\langle a, b\rangle$, c'est-à-dire $\langle\langle a, b\rangle, c\rangle \in f$, alors, au lieu de

$$f(\langle a, b\rangle) = c \quad \text{ou} \quad f(a, b) = c$$

on écrit également

$$afb = c \quad \text{ou} \quad \langle a, b\rangle \mapsto c,$$

l élément c étant appelé *composition d'éléments a et b.*

DÉFINITION. Soit A^n la n-ième puissance de l'ensemble non vide A et $n \geqslant 1$. L'application de l'ensemble A^n dans A est appelée *n-aire opération sur l'ensemble A*, tandis que n est dénommé *rang de l'opération.* L'*opération à aucune place sur l'ensemble A* est appelée séparation (fixation) d'un certain élément de l'ensemble A, le nombre 0 est dénommé *rang de l'opération à aucune place.*

DÉFINITION. L'application de l'ensemble A^n dans A est appelée *opération n-aire partielle sur A* si le domaine de définition de l'application ne coïncide pas avec A^n.

Les opérations de rang 0, 1 et 2 sont également appelées *à aucune place*, *singulaire* (*unaire*) et *binaire* respectivement. L'opération singulaire est aussi dénommée *opérateur.*

E x e m p l e s. 1. L'application associant à chaque ensemble A de $P(M)$ son complémentaire $M \setminus A$ est une *opération singulaire* (*unaire*) *sur un ensemble $P(M)$*.

2. Dans le domaine des nombres naturels la soustraction n'est pas toujours possible. Donc la soustraction sur un ensemble de nombres naturels est une opération binaire partielle.

3. L'opération de division des nombres rationnels est une opération binaire partielle sur un ensemble de nombres rationnels.

4. L'opération associant chaque cortège de n des nombres naturels au plus grand commun diviseur de ces nombres est une opération n-aire sur l'ensemble des nombres naturels.

Pour désigner une opération n-aire on utilise habituellement la même forme de notation que pour des applications (des fonctions) quelconques. Si f est une opération n-aire sur l'ensemble A et

$$\langle\langle a_1, \ldots, a_n\rangle, a_{n+1}\rangle \in f,$$

on écrit $a_{n+1} = f(a_1, \ldots, a_n)$ et l'on dit que a_{n+1} est la valeur de l'opération f pour l'assortiment d'arguments $a_1, \ldots, a_n$.

Types d'opérations binaires. Soient $\top$ et $\perp$ des opérations binaires quelconques sur l'ensemble A.

DÉFINITION. L'opération binaire $\top$ est dite *commutative* si pour tous a, b de A est satisfaite l'égalité $a \top b = b \top a$.

DÉFINITION. L'opération binaire $\top$ est dite *associative* si pour des éléments quelconques a, b, c de A est satisfaite l'égalité $a \top (b \top c) = (a \top b) \top c$.

DÉFINITION. L'opération binaire $\top$ est dite *distributive relativement à l'opération binaire* $\perp$ si pour des a, b, c quelconques de A sont satisfaites les égalités

$$(a \perp b) \top c = (a \top c) \perp (b \top c) \quad \text{et} \quad c \top (a \perp b) = (c \top a) \perp (c \top b).$$

Si l'opération $\top$ est associative, on peut alors supprimer les parenthèses et écrire $a \top b \top c$ au lieu de $a \top (b \top c)$ ou $(a \top b) \top c$.

E x e m p l e s. 1. L'addition et la multiplication des nombres rationnels sont des opérations binaires commutatives et associatives.

2. L'opération de soustraction sur un ensemble de nombres rationnels n'est ni commutative ni associative.

3. Les opérations réunion et intersection de sous-ensembles de l'ensemble M sont commutatives et associatives sur l'ensemble $P(M)$.

4. La composition de fonctions est une opération associative. La composition de fonctions n'est pas commutative: dans le cas général l'égalité $f \circ g = g \circ f$ n'est pas valable.

5. Les opérations réunion et intersection sur un ensemble $P(M)$ de sous-ensembles d'un certain ensemble sont mutuellement distributives l'une par rapport à l'autre.

6. Une multiplication d'entiers est distributive par rapport à l'addition. Or l'addition des entiers n'est pas distributive par rapport à la multiplication, car dans le cas général l'égalité $a + bc = (a + b)(a + c)$ n'est pas valable.

Eléments neutres. Soit $\top$ une opération binaire sur l'ensemble A.

Definition. L'élément e de A est appelé *élément neutre à gauche relativement à l'opération* $\top$ si pour tout a de A est satisfaite l'égalité $e \top a = a$. L'élément e de A est appelé *élément neutre à droite relativement à l'opération* $\top$ si pour tout a de A on a $a \top e = a$.

Definition. L'élément e de A est appelé *élément neutre relativement à l'opération* $\top$ si pour tout élément a de A se vérifient les égalités $e \top a = a = a \top e$.

Théorème 1.1. *S'il existe relativement à l'opération binaire* $\top$ *un élément neutre, il est alors unique.*

Démonstration. Soient e et e' les éléments neutres par rapport à $\top$. Alors, $e' = e' \top e = e$, c'est-à-dire $e' = e$. □

Corollaire 1.2. *S'il existe un élément neutre relativement à l'opération* $\top$, *alors tous les éléments neutres à gauche et à droite par rapport à* $\top$ *coïncident avec lui.*

Exemples. 1. Le nombre 0 est un élément neutre par rapport à l'addition des entiers. Le nombre 1 est un élément neutre par rapport à la multiplication des entiers.

2. Un ensemble vide est un élément neutre relativement à l'opération réunion d'ensembles. Un ensemble universel est un élément neutre relativement à l'opération d'intersection d'ensembles.

3. Considérons l'ensemble Φ d'applications d'un ensemble non vide A sur son sous-ensemble propre non vide B et l'opération composition d'applications. L'ensemble Φ ne comporte aucun élément neutre à droite. Tout élément $\varphi \in \Phi$ tel que $\varphi(x) = x$ pour un x quelconque de B est un élément neutre à gauche relativement à l'opération concernée.

Eléments réguliers. Soit $\top$ une opération binaire sur l'ensemble A.

Definition. L'élément $a \in A$ est appelé *élément régulier à droite relativement à l'opération* $\top$ si pour tous éléments b, c de l'ensemble A il s'ensuit de $a \top b = a \top c$ que $b = c$. L'élément $a \in A$ est appelé *élément régulier à gauche par rapport à* $\top$ si pour tous éléments b, c de l'ensemble A de $b \top a = c \top a$ s'ensuit $b = c$.

Definition. L'élément $a \in A$ est appelé *élément régulier relativement à l'opération* $\top$ s'il est régulier à gauche et à droite par rapport à $\top$.

Ainsi, si l'élément a est régulier dans les égalités du type $a \top b = a \top c$ et $b \top a = c \top a$ on peut simplifier par a.

Exemples. 1. Tout entier est régulier par rapport à une addition.

2. Tout nombre entier différent de zéro est régulier par rapport à une multiplication; le nombre zéro n'est pas régulier par rapport à une multiplication.

Théorème 1.3. *Si les éléments a et b sont réguliers relativement à une opération associative* $\top$, *alors leur composition* $a \top b$ *est également un élément régulier par rapport à* $\top$.

D é m o n s t r a t i o n. Soient a et b les éléments réguliers par rapport à $\top$. Supposons que c, d sont des éléments de A répondant à la condition

(1) $(a \top b) \top c = (a \top b) \top d.$

Puisque l'opération $\top$ est associative, $a \top (b \top c) = a \top (b \top d)$. En vertu de la régularité de l'élément a, on a $b \top c = b \top d$. D'où, en vertu de la régularité de l'élément b, on déduit l'égalité

(2) $c = d.$

Bref, pour tous éléments c, d de l'ensemble A (2) s'ensuit de (1), et par suite, l'élément $a \top b$ est régulier à droite. De façon analogue on se convainc que cet élément est régulier à gauche. □

Eléments symétriques. Soit $\top$ une opération binaire sur l'ensemble A comportant un élément neutre e.

DÉFINITION. L'élément u de A est dit *symétrique à gauche de l'élément $a \in A$* relativement à l'opération $\top$ si $u \top a = e$. L'élément v de A est dit *symétrique à droite de a* relativement à l'opération $\top$ si $a \top v = e$.

DÉFINITION. L'élément $a' \in A$ est appelé *symétrique de l'élément $a \in$ $\in A$* relativement à l'opération $\top$ si $a \top a' = e = a' \top a$. Dans ce cas l'élément a est dit *symétrisable*, tandis que a et a' sont *mutuellement symétriques.*

E x e m p l e s. 1. Par rapport à l'addition d'entiers le symétrique à un entier donné est ce même entier, mais affecté du signe moins.

2. Par rapport à la multiplication de nombres rationnels le symétrique d'un nombre non nul a est $1/a$; le nombre zéro n'a pas de symétrique par rapport à la multiplication.

THÉORÈME 1.4. *Si l'opération $\top$ est associative et l'élément a est symétrisable, il existe alors un élément unique symétrique de a.*

D é m o n s t r a t i o n. Soient u, v les éléments symétriques de l'élément a par rapport à $\top$, c'est-à-dire

$$a \top u = e = u \top a, \quad a \top v = e = v \top a.$$

Alors en vertu de l'associativité de $\top$

$$u = u \top e = u \top (a \top v) = (u \top a) \top v = e \top v = v,$$

c'est-à-dire que $u = v$. □

COROLLAIRE 1.5. *Si l'élément a possède un élément symétrique a' relativement à l'opération associative $\top$, tous les symétriques à gauche et à droite de l'élément a coïncident alors avec l'élément a'.*

THÉORÈME 1.6. *Si les éléments a, b sont symétrisables relativement à l'opération associative $\top$, l'élément $a \top b$, est alors également symétrisable et l'élément $b' \top a'$ est symétrique de $a \top b$.*

D é m o n s t r a t i o n. Soient a' et b' les éléments symétriques de a et b respectivement. En vertu de l'associativité de $\top$

$$(a \top b) \top (b' \top a') = ((a \top b) \top b') \top a' = (a \top (b \top b')) \top a' =$$
$$= (a \top e) \top a' = a \top a' = e.$$

On se convainc de même que $(b' \top a') \top (a \top b) = e$. Par conséquent, l'élément $a \top b$ est symétrisable et l'élément $b' \top a'$ est symétrique de $a \top b$. □

THÉORÈME 1.7. *Un élément symétrisable relativement à une opération associative* $\top$ *est un élément régulier par rapport à* $\top$.

D é m o n s t r a t i o n. Soient a un élément symétrisable et $a \top b = a \top c$ pour les éléments b, c de l'ensemble A. Dans ce cas si a' est un élément symétrique de a, on a $a' \top (a \top b) = a' \top \top (a \top c)$. En vertu de l'associativité de l'opération $\top$, on a $(a' \top \top a) \top b = (a' \top a) \top c$. Par conséquent, $e \top b = e \top c$ et $b = = c$. On se convainc de façon analogue que pour tous éléments b, c de l'ensemble A de l'égalité $b \top a = c \top a$ s'ensuit $b = c$. L'élément a est donc régulier par rapport à $\top$. □

Sous-ensembles fermés aux opérations. Soient $\top$ une opération binaire sur un ensemble A et $B \subset A$.

DÉFINITION. Le sous-ensemble B de l'ensemble A est dit *fermé à l'opération* $\top$ si pour tous a, b de B l'élément $a \top b$ appartient à B.

Notons qu'un sous-ensemble vide est fermé à toute opération $\top$.

E x e m p l e s. 1. L'ensemble de tous les nombres pairs est fermé par rapport à l'addition et à la multiplication des entiers.

2. L'ensemble de tous les nombres impairs est fermé par rapport à la multiplication, mais ne l'est pas par rapport à l'addition des entiers.

3. L'ensemble de tous les éléments (de A) réguliers relativement à l'opération associative $\top$ est fermé par rapport à $\top$.

PROPOSITION 1.8. *L'ensemble de tous les éléments symétrisables relativement à une opération binaire associative* $\top$ *est fermé par rapport à* $\top$.

La démonstration de cette proposition découle directement du théorème 1.6.

Soit B un ensemble non vide, $B \subset A$ étant fermé à l'opération $\top$. On est alors en mesure de définir sur B une opération binaire $\top'$ de la façon suivante:

$$a \top' b = a \top b \text{ pour } a, b \text{ de } B \text{ quelconques.}$$

L'opération $\top'$ est appelée *restriction de l'opération* $\top$ *à l'ensemble* B, tandis que $\top$ est le *prolongement de l'opération* $\top'$ *à l'ensemble* A.

Ecritures additive et multiplicative. Les écritures le plus souvent utilisées pour une opération binaire sont les écritures additive et multiplicative. Avec la forme d'écriture additive l'opération binaire $\top$ est appelée *addition* et l'on écrit $a + b$ au lieu de $a \top b$ en appelant l'élément $a + b$ somme de a et b. L'élément symétrique de l'élément a est désigné $(-a)$ et est appelé *élément opposé à a*. Un élément neutre par rapport à l'addition est noté 0 et appelé *élément zéro* par rapport à l'addition. Avec la notation additive les propriétés d'associativité et de commutativité se notent sous la forme

$$a + (b + c) = (a + b) + c, \qquad a + b = b + a.$$

Avec l'écriture multiplicative l'opération binaire est appelée *multiplication* et l'on écrit $a \cdot b$ (au lieu de $a \top b$) en appelant l'élément $a \cdot b$ produit de a et b. L'élément symétrique de a est noté a^{-1} et s'appelle *élément inverse de a*. Un élément neutre par rapport à la multiplication est noté e ou 1 et est dénommé *élément unitaire* ou *élément unité par rapport à la multiplication*. Avec l'écriture multiplicative les propriétés d'associativité et de commutativité se notent ainsi

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, \qquad a \cdot b = b \cdot a.$$

La propriété de distributivité de la multiplication par rapport à l'addition s'écrit ainsi

$$(a + b) \cdot c = a \cdot c + b \cdot c, \qquad c\,(a + b) = c \cdot a + c \cdot b.$$

Congruence. Soient R une relation d'équivalence sur l'ensemble A et $\top$ une opération binaire sur A.

DEFINITION. Une relation d'équivalence R est appelée *congruence relativement à l'opération* $\top$ si pour tous éléments a, b, c, d de l'ensemble A de aRc et bRd s'ensuit $(a \top b)\ R\ (c \top d)$.

THEOREME 1.9. *Soient* $\top$ *une opération binaire sur un ensemble A et R une congruence par rapport à* $\top$. *Alors, l'égalité*

(1) $\quad (a/R) \top^* (b/R) = (a \top b)/R,$

où a, $b \in A$, *définit l'opération binaire* $\top^*$ *sur l'ensemble quotient* A/R.

D é m o n s t r a t i o n. La relation binaire $\top^*$ comporte deux couples de la forme

(2) $\quad \langle\langle a/R,\ b/R\rangle,\ (a \top b)/R\rangle, \quad$ où $\quad a,\ b \in A.$

On doit démontrer que $\top^*$ est une fonction. Soit

$$\langle\langle c/R,\ d/R\rangle,\ (c \top d)/R\rangle \in \top^*.$$

On doit montrer que de l'égalité

(3) $\quad \langle a/R,\ b/R\rangle = \langle c/R,\ d/R\rangle$

s'ensuit $(a \top b)/R = (c \top d)/R$. De (3) découlent les égalités $a/R = c/R$, $b/R = d/R$ et les relations

(4) aRc, bRd.

Vu que R est une congruence par rapport à $\top$, de (4) s'ensuit:

$$(a \top b)\ R\ (c \top d) \quad \text{et} \quad (a \top b)/R = (c \top d)/R.$$

Par conséquent, la relation $\top^*$ est une opération binaire sur l'ensemble quotient A/R. □

DÉFINITION. Une opération binaire $\top^*$ définie sur un ensemble quotient A/R par l'égalité (1) est appelée *opération associée à l'opération* $\top$ *par la congruence* R.

Exercices

1. Soient $\mathbf{N}^*$ l'ensemble de tous les entiers positifs et $\top$ l'opération sur $\mathbf{N}^*$ d'élévation à une puissance, c'est-à-dire que $a \top b = a^b$ pour tous $a, b \in \mathbf{N}^*$. Montrer que l'opération $\top$ n'est ni commutative ni associative.

2. Soient a, b des nombres rationnels fixés. Montrer que l'application $\langle x, y\rangle \mapsto ax + by$, où x, y sont des nombres rationnels quelconques, est une opération binaire associative sur l'ensemble des nombres rationnels.

3. Soient $\mathbf{N}$ l'ensemble de tous les nombres naturels et (x, y) le plus grand commun diviseur des nombres naturels x et y. Démontrer que l'application $\langle x, y\rangle \mapsto (x, y)$ est une opération binaire commutative et associative sur l'ensemble $\mathbf{N}$.

4. Soient $[x, y]$ le plus petit commun multiple des nombres naturels x et y. Montrer que l'application $\langle x, y\rangle \mapsto [x, y]$ est une opération commutative et associative sur l'ensemble $\mathbf{N}$.

5. Soit $P(U)$ un ensemble de tous les sous-ensembles de l'ensemble non vide U. L'ensemble $X \Delta Y$ défini par la formule

$$X \Delta Y = (X \setminus Y) \cup (Y \setminus X)$$

est appelé *différence symétrique des ensembles* X et Y. Démontrer que Δ est une opération binaire commutative et associative sur l'ensemble $P(U)$. Montrer que l'opération $\cap$ est distributive relativement à l'opération Δ.

6. Donner un exemple d'ensemble A, de relation d'équivalence R sur A et d'opération binaire $\top$ sur A tels que

(a) R soit une congruence par rapport à $\top$,

(b) R ne soit pas une congruence par rapport à $\top$.

§ 2. Algèbres

Notion d'algèbre. Donnons la définition d'une notion fondamentale en algèbre.

DÉFINITION. On appelle *algèbre* un couple ordonné $\mathcal{A} = \langle A, \Omega\rangle$, où A est un ensemble non vide et Ω l'ensemble des opérations sur A.

Ainsi donc l'algèbre $\mathcal{A}$ se définit par deux ensembles:

(a) un ensemble non vide A noté également $|\mathcal{A}|$; cet ensemble est appelé *ensemble fondamental* (*ensemble de base*) *de l'algèbre* $\mathcal{A}$ et ses éléments s'appellent *éléments de l'algèbre* $\mathcal{A}$;

(b) un ensemble d'opérations Ω définies sur A et appelées *opérations principales de l'algèbre* $\mathcal{A}$.

Si $\langle A, \Omega\rangle$ est une algèbre, on dit de même que l'ensemble A est une algèbre relativement aux opérations Ω.

DEFINITION. Les algèbres $\mathcal{A} = \langle A, \Omega\rangle$ et $\mathcal{B} = \langle B, \Omega'\rangle$ sont dites *du même type* s'il existe une application injective de l'ensemble Ω sur Ω' pour laquelle toute opération $f_{\mathcal{A}}$ de Ω et l'opération $f_{\mathcal{B}}$ de Ω', qui lui correspond dans l'application, possèdent le même rang.

Le cas le plus général est celui où l'ensemble Ω est fini, c'est-à-dire $\Omega = \{f_1, \ldots, f_s\}$. Dans ce cas au lieu de la notation

$$\mathcal{A} = \langle A, \{f_1, \ldots, f_s\}\rangle$$

on écrit habituellement

$$\mathcal{A} = \langle A, f_1, \ldots, f_s\rangle.$$

Si parmi les opérations principales $f_1, \ldots, f_s$ de l'algèbre il y a des opérations à aucune place, par exemple, $f_{r+1}, \ldots, f_s$, et $a_{r+1}, \ldots, a_s$ étant des éléments séparés de $|\mathcal{A}|$, on utilise aussi la notation

$$\mathcal{A} = \langle A, f_1, \ldots, f_r, a_{r+1}, \ldots, a_s\rangle.$$

Dans ce cas les éléments séparés $a_{r+1}, \ldots, a_s$ constituant les valeurs des opérations principales à aucune place sont appelés *éléments séparés* ou *éléments principaux de l'algèbre* $\mathcal{A}$.

On appelle *type d'algèbre* $\mathcal{A} = \langle A, f_1, \ldots, f_s\rangle$ la suite $(r(f_1), \ldots$ $\ldots, r(f_s))$, où $r(f_i)$ est le *rang de l'opération* f_i. Les algèbres $\mathcal{A}$ et $\mathcal{B} = \langle B, f'_1, \ldots, f'_s\rangle$ sont du même type en cas de coïncidence, c'est-à-dire au cas où le rang de l'opération f_i coïncide avec le rang de l'opération f'_i pour $i = 1, \ldots, s$.

E x e m p l e s. 1. Soient $+$ et $\cdot$ (addition et multiplication) des opérations arithmétiques sur l'ensemble **Z** des entiers. L'algèbre $\langle \mathbf{Z}, +, \cdot\rangle$ est une algèbre du type (2, 2).

2. Soient $+$ et $\cdot$ des opérations arithmétiques sur l'ensemble **N** des nombres naturels. L'algèbre $\langle \mathbf{N}, +, \cdot\rangle$ est une algèbre du type (2, 2).

3. Soient $P(U)$ un ensemble de tous les sous-ensembles d'un ensemble non vide U et $\cap$, $\cup$, $'$ des opérations intersection, réunion et complémentation sur les sous-ensembles de l'ensemble U. L'algèbre $\langle P(U), \cap, \cup, '\rangle$ est une algèbre du type (2, 2, 1).

DEFINITION. Une algèbre $\mathcal{A} = \langle A, *, e\rangle$ du type (2, 0), où A est un ensemble quelconque non vide, $*$ une opération binaire associative sur A, e un élément neutre par rapport à $*$, est dénommée *monoïde*.

E x e m p l e. Soient M un ensemble fini quelconque non vide, A l'ensemble de toutes les applications de M dans M, $*$ une opéra-

tion de composition d'applications de M dans M, i_M une application identique de M dans M. Alors, $\langle A, *, i_A \rangle$ est un monoïde.

Homomorphismes d'algèbres. Soient $\mathcal{A}$ et $\mathcal{B}$ des algèbres du même type, $f_{\mathcal{A}}$ une opération principale quelconque de l'algèbre $\mathcal{A}$ et $f_{\mathcal{B}}$ l'opération principale qui lui correspond dans l'algèbre $\mathcal{B}$. On dit que l'application h de l'ensemble $|\mathcal{A}|$ dans l'ensemble $|\mathcal{B}|$ respecte l'opération $f_{\mathcal{A}}$ de l'algèbre $\mathcal{A}$ si

$$(1) \quad h(f_{\mathcal{A}}(a_1, \ldots, a_m)) = f_{\mathcal{B}}(h(a_1), \ldots, h(a_m)) \quad \text{pour tous } a_1, \ldots, a_m \text{ de } |\mathcal{A}|,$$

où m est le rang de l'opération $f_{\mathcal{A}}$.

Distinguons le cas où $f_{\mathcal{A}}$ est une opération à aucune place, c'est-à-dire qu'elle sépare un élément quelconque a de l'algèbre $\mathcal{A}$. L'opération $f_{\mathcal{B}}$ qui lui correspond sera alors également une opération à aucune place et, partant, séparera un élément quelconque b de l'algèbre $\mathcal{B}$. Dans ce cas la condition (1) prendra la forme

$$h(a) = b,$$

c'est-à-dire que l'élément séparé a de l'algèbre $\mathcal{A}$ devient dans l'application h l'élément séparé b de l'algèbre $\mathcal{B}$.

DÉFINITION. On appelle *homomorphisme de l'algèbre* $\mathcal{A}$ dans (sur) l'algèbre du même type $\mathcal{B}$ une telle application h de l'ensemble $|\mathcal{A}|$ dans (sur) $|\mathcal{B}|$ qui respecte toutes les opérations principales de l'algèbre $\mathcal{A}$, c'est-à-dire qui satisfait à la condition (1) pour toute opération principale $f_{\mathcal{A}}$ de l'algèbre $\mathcal{A}$. L'homomorphisme de l'algèbre $\mathcal{A}$ sur $\mathcal{B}$ est appelé *épimorphisme*.

DÉFINITION. L'homomorphisme h de l'algèbre $\mathcal{A}$ sur l'algèbre $\mathcal{B}$ est dénommé *isomorphisme* si h est une application injective de l'ensemble $|\mathcal{A}|$ sur $|\mathcal{B}|$. Les algèbres $\mathcal{A}$ et $\mathcal{B}$ sont dites *isomorphes* s'il y a isomorphisme de $\mathcal{A}$ sur $\mathcal{B}$.

La notation $\mathcal{A} \cong \mathcal{B}$ signifie que les algèbres $\mathcal{A}$ et $\mathcal{B}$ sont isomorphes.

DÉFINITION. L'homomorphisme h de l'algèbre $\mathcal{A}$ dans l'algèbre $\mathcal{B}$ est appelé *monomorphisme* ou *injection* si h est une application injective de l'ensemble $|\mathcal{A}|$ dans $|\mathcal{B}|$.

DÉFINITION. L'homomorphisme de l'algèbre $\mathcal{A}$ en elle-même est appelé *endomorphisme de l'algèbre* $\mathcal{A}$. L'isomorphisme de l'algèbre $\mathcal{A}$ sur elle-même s'appelle *automorphisme de l'algèbre* $\mathcal{A}$.

Ainsi, par exemple, l'automorphisme de l'algèbre $\mathcal{A}$ est une application identique de l'ensemble $|\mathcal{A}|$ sur lui-même.

Exemple. Soient $+$ l'opération d'addition sur l'ensemble **R** des nombres réels et $\cdot$ l'opération de multiplication sur l'ensemble $\mathbf{R}^*$ des nombres réels positifs. Chacune des algèbres $\langle \mathbf{R}^*, \cdot, 1 \rangle$ et $\langle \mathbf{R}, +, 0 \rangle$ est du type (2, 0). Montrons qu'elles sont isomorphes.

Considérons l'application h:

$h(x) = \log x$ pour tout x de $\mathbf{R}^*$.

On voit sans peine que h est l'application de $\mathbf{R}^*$ sur $\mathbf{R}$. L'application h est injective, car pour tous x, y de $\mathbf{R}^*$ est satisfaite la condition : si $\log x = \log y$, alors $x = y$. En outre, $h(1) = 0$ et pour tous x, y de $\mathbf{R}^*$ on a $\log(xy) = \log x + \log y$, c'est-à-dire que $h(x, y) = h(x) + h(y)$. Donc, l'application h respecte les principales opérations de l'algèbre $\langle \mathbf{R}^*, \cdot, 1 \rangle$. Par conséquent, h est un isomorphisme de la première algèbre sur la seconde.

THÉORÈME 2.1. *Soient h un homomorphisme de l'algèbre $\mathcal{A}$ dans l'algèbre $\mathcal{B}$ et g un homomorphisme de l'algèbre $\mathcal{B}$ dans l'algèbre $\mathcal{C}$. Leur composition $g \circ h$ est alors un homomorphisme de l'algèbre $\mathcal{A}$ dans l'algèbre $\mathcal{C}$.*

Démonstration. Soient $f_{\mathcal{A}}$ une opération principale quelconque de l'algèbre $\mathcal{A}$ (de rang $m > 0$), $f_{\mathcal{B}}$ l'opération principale associée de l'algèbre $\mathcal{B}$ et $f_{\mathcal{C}}$ l'opération principale de l'algèbre $\mathcal{C}$ correspondant à l'opération $f_{\mathcal{B}}$. Il faut démontrer que pour tous éléments $a_1, \ldots, a_m$ de $|\mathcal{A}|$, on a

$$(1) \quad g \circ h\,(f_{\mathcal{A}}(a_1, \ldots, a_m)) = f_{\mathcal{C}}(g \circ h\,(a_1), \ldots, g \circ h\,(a_m)).$$

Par définition de la composition d'applications

$$g \circ h\,(f_{\mathcal{A}}(a_1, \ldots, a_m)) = g\,(h\,(f_{\mathcal{A}}(a_1, \ldots, a_m))).$$

Or, comme par hypothèse h et g sont des homomorphismes, on a

$$\begin{aligned} g\,(h\,(f_{\mathcal{A}}(a_1, \ldots, a_m))) &= g\,(f_{\mathcal{B}}(h\,(a_1), \ldots, h\,(a_m))) = \\ &= f_{\mathcal{C}}(g\,(h\,(a_1)), \ldots, g\,(h\,(a_m))) = \\ &= f_{\mathcal{C}}((g \circ h)\,(a_1), \ldots, (g \circ h)\,(a_m)). \end{aligned}$$

Par conséquent, l'égalité (1) est vérifiée. Pour des opérations principales à aucune place les raisonnements sont identiques. □

Théorème 2.2. *Soient h un homomorphisme de l'algèbre $\mathcal{A}$ sur l'algèbre $\mathcal{B}$ et g un homomorphisme de l'algèbre $\mathcal{B}$ sur l'algèbre $\mathcal{C}$. Leur composition $g \circ h$ est alors un homomorphisme de l'algèbre $\mathcal{A}$ sur l'algèbre $\mathcal{C}$.*

Ce théorème découle directement du théorème 2.1 et du théorème 2.3.4.

THÉORÈME 2.3. *Soient h un isomorphisme de l'algèbre $\mathcal{A}$ sur l'algèbre $\mathcal{B}$ et g un isomorphisme de l'algèbre $\mathcal{B}$ sur l'algèbre $\mathcal{C}$. Leur composition $g \circ h$ est alors un isomorphisme de l'algèbre $\mathcal{A}$ sur l'algèbre $\mathcal{C}$.*

Démonstration. Selon le théorème 2.1 il découle de l'hypothèse que $g \circ h$ est un homomorphisme de l'algèbre $\mathcal{A}$ dans

l'algèbre $\mathscr{C}$. Ensuite, par hypothèse h est une application injective de l'ensemble $|\mathscr{A}|$ sur $|\mathscr{B}|$ et g une application injective de l'ensemble $|\mathscr{B}|$ sur $|\mathscr{C}|$. Selon les théorèmes 2.3.9 et 2.3.4 il s'ensuit que $g \circ h$ est une application injective de l'ensemble $|\mathscr{A}|$ sur $|\mathscr{C}|$. Donc $g \circ h$ est un isomorphisme de l'algèbre $\mathscr{A}$ sur l'algèbre $\mathscr{C}$. □

THÉORÈME 2.4. *Soit h un isomorphisme de l'algèbre $\mathscr{A}$ sur l'algèbre $\mathscr{B}$. L'application h^{-1} est alors un isomorphisme de l'algèbre $\mathscr{B}$ sur l'algèbre $\mathscr{A}$.*

D é m o n s t r a t i o n. Par hypothèse h est une application injective de l'ensemble $|\mathscr{A}|$ sur $|\mathscr{B}|$. Aussi, selon le corollaire 2.3.14, h^{-1} est-il une application injective de $|\mathscr{B}|$ sur $|\mathscr{A}|$. Soient $f_{\mathscr{A}}$ une opération principale quelconque de l'algèbre $\mathscr{A}$ (de rang m) et $f_{\mathscr{B}}$ une opération principale appropriée de l'algèbre $\mathscr{B}$. Il nous suffit de démontrer que pour tous éléments $b_1, \ldots, b_m$ de $|\mathscr{B}|$, on a

$$(1) \quad h^{-1}(f_{\mathscr{B}}(b_1, \ldots, b_m)) = f_{\mathscr{A}}(h^{-1}(b_1), \ldots, h^{-1}(b_m)).$$

Cette condition est équivalente à la suivante:

$$(2) \quad h(f_{\mathscr{A}}(h^{-1}(b_1), \ldots, h^{-1}(b_m))) = f_{\mathscr{B}}(b_1, \ldots, b_m).$$

Or, comme par hypothèse h est un homomorphisme de l'algèbre $\mathscr{A}$ sur $\mathscr{B}$, on a

$$h(f_{\mathscr{A}}(h^{-1}(b_1), \ldots, h^{-1}(b_m))) = f_{\mathscr{B}}(h(h^{-1}(b_1)), \ldots$$
$$\ldots, h(h^{-1}(b_m))) = f_{\mathscr{B}}(b_1, \ldots, b_m),$$

c'est-à-dire que (2) est vérifiée et, partant, (1) l'est aussi. Par conséquent, h^{-1} est un isomorphisme de l'algèbre $\mathscr{B}$ sur l'algèbre $\mathscr{A}$. □

THÉORÈME 2.5. *Une relation d'isomorphisme sur un ensemble quelconque d'algèbres est une relation d'équivalence.*

D é m o n s t r a t i o n. Une application identique de l'algèbre $\mathscr{A}$ sur l'algèbre $\mathscr{A}$, c'est-à-dire une application h telle que $h(a) = a$ quel que soit a de $|\mathscr{A}|$, est apparemment un isomorphisme de l'algèbre $\mathscr{A}$ sur $\mathscr{A}$. Selon le théorème 2.3 la relation d'isomorphisme est transitive. Selon le théorème 2.4 la relation d'isomorphisme est symétrique. Donc, la relation d'isomorphisme est une relation d'équivalence. □

Sous-algèbres. Soient f une opération n-aire sur l'ensemble A et B un sous-ensemble non vide de l'ensemble A. En accord avec la notion de restriction d'une fonction à un ensemble on dit qu'une opération n-aire g sur B est une restriction de l'opération f à l'ensemble B si

$$g(b_1, \ldots, b_n) = f(b_1, \ldots, b_n) \text{ pour tous } b_1, \ldots, b_n \text{ de } B.$$

En particulier, une opération à aucune place g sur B est une restriction de l'opération à aucune place f sur A à l'ensemble B, si

$g = f$, c'est-à-dire si g et f séparent un même élément respectivement dans B et A. La restriction de l'opération f par l'ensemble B sera désignée par le symbole $f \mid B$.

Soient $\mathcal{A} = \langle A, \Omega \rangle$ et $\mathcal{B} = \langle B, \Omega' \rangle$ des algèbres du même type.

DÉFINITION. L'algèbre $\mathcal{B}$ est appelée *sous-algèbre* d'une algèbre du même type $\mathcal{A}$ si $B \subset A$ et l'application identique de l'ensemble B dans A est un monomorphisme de l'algèbre $\mathcal{B}$ dans l'algèbre $\mathcal{A}$, c'est-à-dire pour chaque opération principale $f_{\mathcal{B}}$ de l'algèbre $\mathcal{B}$ on a

$$f_{\mathcal{B}}(b_1, \ldots, b_m) = f_{\mathcal{A}}(b_1, \ldots, b_m) \quad \textit{pour tous } b_1, \ldots, b_m \textit{ de } B,$$

où m est le rang de l'opération $f_{\mathcal{A}}$, tandis que $f_{\mathcal{B}}$ est l'opération principale de l'algèbre $\mathcal{B}$ correspondant à $f_{\mathcal{A}}$.

Rappelons que par application identique de l'ensemble B dans A on entend une application h telle que $h(b) = b$ quel que soit l'élément b de B.

On montre sans peine que la définition de la sous-algèbre donnée plus haut est équivalente à l'énoncé suivant: l'algèbre $\mathcal{B}$ est appelée *sous-algèbre* de l'algèbre du même type $\mathcal{A}$ si $B \subset A$ et chaque opération principale $f_{\mathcal{B}}$ de l'algèbre $\mathcal{B}$ est une restriction de l'opération correspondante $f_{\mathcal{A}}$ de l'algèbre $\mathcal{A}$ à l'ensemble B.

La notation $\mathcal{B} \dashv \mathcal{A}$ signifie que l'algèbre $\mathcal{B}$ est une sous-algèbre de l'algèbre $\mathcal{A}$.

Soient $\mathcal{A} = \langle A, \Omega \rangle$ une algèbre et $B \subset A$.

DÉFINITION. Un sous-ensemble B de l'ensemble $|\mathcal{A}|$ est dit *clos dans l'algèbre* $\mathcal{A}$ si B est clos relativement à chaque opération principale $f_{\mathcal{A}}$ de l'algèbre $\mathcal{A}$, c'est-à-dire si l'on a

$$(1) \quad f_{\mathcal{A}}(b_1, \ldots, b_m) \in B \quad \textit{pour tous } b_1, \ldots, b_m \textit{ de } B,$$

où m est le rang de l'opération $f_{\mathcal{A}}$. Si $f_{\mathcal{A}}$ est une opération à aucune place, la condition (1) prend la forme $f_{\mathcal{A}} \in B$.

Il va de soi que si $\mathcal{B} \dashv \mathcal{A}$, alors l'ensemble $|\mathcal{B}|$ est clos dans l'algèbre $\mathcal{A}$.

A partir des définitions fournies plus haut découle directement le théorème suivant.

THÉORÈME 2.6. *Soient* $\mathcal{A} = \langle A, f_1, \ldots, f_s \rangle$ *une algèbre et* B *un sous-ensemble non vide de l'ensemble* A *clos dans l'algèbre* $\mathcal{A}$. *Dans ce cas l'algèbre*

$$(2) \quad \mathcal{B} = \langle B, f_1 \mid B, \ldots, f_s \mid B \rangle$$

est une sous-algèbre de l'algèbre $\mathcal{A}$.

Puisque le sous-ensemble non vide B de l'ensemble $|\mathcal{A}|$ clos dans l'algèbre $\mathcal{A}$ définit de façon univoque (de manière susmentionnée) la sous-algèbre $\mathcal{B}$, on utilise pour cette sous-algèbre au lieu de

la notation (2) la notation

$\mathcal{B} = \langle B, f_1, \ldots, f_s \rangle$.

Exemples. 1. Soient $+$ et $\cdot$ (addition et multiplication) les opérations arithmétiques usuelles sur l'ensemble **Z** des entiers et **N** un ensemble des nombres naturels. Dans ce cas l'algèbre $\langle \mathbf{N}, +, \cdot \rangle$ est alors une sous-algèbre de l'algèbre $\langle \mathbf{Z}, +, \cdot \rangle$.

2. Soit $P(U)$ l'ensemble de tous les sous-ensembles de l'ensemble non vide U, tandis que $\cap$, $\cup$ et $'$ sont respectivement les opérations intersection, réunion et complémentation. L'algèbre $\langle \{\varnothing, U\}, \cap, \cup, ' \rangle$ est une sous-algèbre de l'algèbre $\langle P(U), \cap, \cup, ' \rangle$.

THÉORÈME 2.7. *Si $\mathcal{A}$ est une sous-algèbre de l'algèbre $\mathcal{B}$ et $\mathcal{B}$ une sous-algèbre de l'algèbre $\mathcal{C}$, $\mathcal{A}$ est alors une sous-algèbre de l'algèbre $\mathcal{C}$.*

Démonstration. Soit $\mathcal{A} \dashv \mathcal{B}$. Dans ce cas $|\mathcal{A}| \subset \subset |\mathcal{B}|$ et

(1) $f_{\mathcal{A}}(a_1, \ldots, a_m) = f_{\mathcal{B}}(a_1, \ldots, a_m)$

pour tous $a_1, \ldots, a_m$ de $|\mathcal{A}|$,

où $f_{\mathcal{A}}$ est une opération principale quelconque de l'algèbre $\mathcal{A}$ et m son rang, tandis que $f_{\mathcal{B}}$ est l'opération appropriée de l'algèbre $\mathcal{B}$. Ensuite, si $\mathcal{B} \dashv \mathcal{C}$, on a $|\mathcal{B}| \subset |\mathcal{C}|$ et

(2) $f_{\mathcal{B}}(a_1, \ldots, a_m) = f_{\mathcal{C}}(a_1, \ldots, a_m)$

pour tous $a_1, \ldots, a_m$ de $|\mathcal{B}|$,

où $f_{\mathcal{C}}$ est l'opération principale de l'algèbre $\mathcal{C}$ correspondant à l'opération $f_{\mathcal{B}}$. Aussi a-t-on $|\mathcal{A}| \subset |\mathcal{C}|$ et en vertu de (1), (2)

$f_{\mathcal{A}}(a_1, \ldots, a_m) = f_{\mathcal{C}}(a_1, \ldots, a_m)$

pour tous $a_1, \ldots, a_m$ de $|\mathcal{A}|$.

Par conséquent, $\mathcal{A}$ est une sous-algèbre de l'algèbre $\mathcal{C}$. □

THÉORÈME 2.8. *La relation binaire $\dashv$ (« être une sous-algèbre ») sur l'ensemble des sous-algèbres de l'algèbre $\mathcal{A}$ est une relation d'ordre non strict.*

Démonstration. Une application identique de l'ensemble $|\mathcal{A}|$ sur $|\mathcal{A}|$ est un monomorphisme de l'algèbre $\mathcal{A}$ sur $\mathcal{A}$. Par conséquent, $\mathcal{A} \dashv \mathcal{A}$, la relation $\dashv$ est donc réflexive. En vertu du théorème 2.7 la relation $\dashv$ est transitive.

Montrons que la relation $\dashv$ est antisymétrique. Admettons que les sous-algèbres $\mathcal{B}$ et $\mathcal{C}$ de l'algèbre $\mathcal{A}$ satisfont aux conditions

(1) $\mathcal{B} \dashv \mathcal{C}$ et $\mathcal{C} \dashv \mathcal{B}$.

Alors $|\mathcal{B}| \subset |\mathcal{C}|$, $|\mathcal{C}| \subset |\mathcal{B}|$ et, par suite,

(2) $|\mathcal{B}| = |\mathcal{C}|$.

Ensuite, en vertu de (1) pour une opération principale quelconque $f_{\mathcal{B}}$ de l'algèbre $\mathcal{B}$ on a

(3) $f_{\mathcal{B}}(b_1, \ldots, b_m) = f_{\mathcal{C}}(b_1, \ldots, b_m)$

pour tous $b_1, \ldots, b_m$ de $|\mathcal{B}|$,

où m est le rang de l'opération $f_{\mathcal{B}}$. En vertu de (2) et (3) on a

(4) $f_{\mathcal{B}} = f_{\mathcal{C}}$ pour toute opération principale $f_{\mathcal{B}}$ de l'algèbre $\mathcal{B}$.

Sur la base de (2) et (4) on conclut que $\mathcal{B} = \mathcal{C}$. Donc, la relation $\dashv$ est antisymétrique.

Bref, il est établi que la relation $\dashv$ est réflexive, transitive et antisymétrique, c'est donc une relation d'ordre non strict. □

Théorème 2.9. *L'intersection d'une collection quelconque de sous-ensembles de l'ensemble* $|\mathcal{A}|$ *clos dans l'algèbre* $\mathcal{A}$ *est un ensemble clos dans l'algèbre* $\mathcal{A}$.

Démonstration. Soient $\{C_i \mid i \in \mathrm{I}\}$ une collection quelconque des sous-ensembles C_i de l'ensemble $|\mathcal{A}|$ clos dans l'algèbre $\mathcal{A}$ et $C = \bigcap_{i \in \mathrm{I}} C_i$. Si $C = \varnothing$ le théorème est vérifié car un ensemble vide est clos dans $\mathcal{A}$. Voyons le cas où $C \neq \varnothing$. Soient $f_{\mathcal{A}}$ une opération principale quelconque de l'algèbre $\mathcal{A}$, m son rang et $c_1, \ldots, c_m$ des éléments quelconques de l'ensemble C. Dans ce cas

(1) $f_{\mathcal{A}}(c_1, \ldots, c_m) \in C_i$ pour chaque i de I,

vu que l'ensemble C_i est clos relativement à l'opération $f_{\mathcal{A}}$. En vertu de (1)

$$f_{\mathcal{A}}(c_1, \ldots, c_m) \in \bigcap_{i \in \mathrm{I}} C_i = C,$$

c'est-à-dire que l'ensemble C est clos relativement à toutes les opérations principales de l'algèbre $\mathcal{A}$. □

Soit $\mathcal{A}$ une algèbre

(I) $\{\mathcal{A}_i \mid i \in \mathrm{I}\}$

une collection quelconque des sous-algèbres $\mathcal{A}_i$ de l'algèbre $\mathcal{A}$ telle que $\bigcap_{i \in \mathrm{I}} |\mathcal{A}_i|$ soit un ensemble non vide.

Définition. On appelle *intersection de la collection* (I) des sous-algèbres de l'algèbre $\mathcal{A}$ la sous-algèbre $\mathcal{B}$ de l'algèbre $\mathcal{A}$ telle que $|\mathcal{B}| = \bigcap_{i \in \mathrm{I}} |\mathcal{A}_i|$.

Le bien-fondé de cette définition découle du fait que (en vertu du théorème 2.9) l'ensemble $|\mathcal{B}| = \bigcap_{i \in \mathrm{I}} |\mathcal{A}_i|$ est clos dans l'algèbre $\mathcal{A}$ et le sous-ensemble $|\mathcal{B}|$ non vide et clos dans l'algèbre $\mathcal{A}$ de l'ensemble $|\mathcal{A}|$ (en vertu du théorème 2.6) définit de façon unique la sous-algèbre de l'algèbre $\mathcal{A}$ à ensemble de base $|\mathcal{B}|$.

La notation $\mathscr{B} = \bigcap_{i \in I} \mathscr{A}_i$ signifie que l'algèbre $\mathscr{B}$ est une intersection de la collection (I) des sous-algèbres $\mathscr{A}_i$ de l'algèbre $\mathscr{A}$.

Bref, si (I) est une collection quelconque des sous-algèbres de l'algèbre $\mathscr{A} = \langle A, f_1, \ldots, f_s \rangle$ telle que $\bigcap_{i \in I} | \mathscr{A}_i | \neq \varnothing$, l'algèbre $\mathscr{B}$

$$\mathscr{B} = \langle B, f_1 \mid B, \ldots, f_s \mid B \rangle,$$

où $B = \bigcap_{i \in I} | \mathscr{A}_i |$, est alors l'intersection des algèbres de la collection (I).

Théorème 2.10. *Si dans l'algèbre $\mathscr{A}$ parmi les opérations principales on rencontre au moins une à aucune place, l'intersection d'une collection quelconque (non vide) des sous-algèbres de l'algèbre $\mathscr{A}$ est alors une sous-algèbre de l'algèbre $\mathscr{A}$.*

Démonstration. En effet, si $\{\mathscr{A}_i \mid i \in I\}$ est une collection quelconque des sous-algèbres de l'algèbre $\mathscr{A}$ comportant au moins une opération principale à aucune place $f_{\mathscr{A}}$, l'ensemble $B = \bigcap_{i \in I} | \mathscr{A}_i |$ est alors non vide, car il contient un élément séparé par l'opération $f_{\mathscr{A}}$. Dans ce cas l'ensemble B clos dans $\mathscr{A}$ définit (en vertu du théorème 2.6) de façon unique la sous-algèbre de l'algèbre $\mathscr{A}$ à ensemble de base B. □

Il s'ensuit de la définition de la sous-algèbre que pour tout ensemble non vide M d'éléments de l'algèbre $\mathscr{A}$ donnée, $M \subset | \mathscr{A} |$, il existe une sous-algèbre minimale $\mathscr{B}$ incluant M. On constate sans peine qu'une telle sous-algèbre est l'intersection de toutes les sous-algèbres de l'algèbre $\mathscr{A}$ comportant l'ensemble M. Cette sous-algèbre minimale $\mathscr{B}$ est dénommée *sous-algèbre engendrée par l'ensemble M*, M étant un système de génératrices de l'algèbre $\mathscr{B}$.

Algèbre quotient. Soient $\mathscr{A}$ une algèbre et R une relation d'équivalence sur l'ensemble $| \mathscr{A} |$.

Définition. La relation R est appelée *congruence* ou *congruence dans l'algèbre $\mathscr{A}$* si R est une congruence relativement à chaque opération principale $f_{\mathscr{A}}$ de l'algèbre $\mathscr{A}$, c'est-à-dire que pour tous éléments $a_1, b_1, \ldots, a_m, b_m$ de l'ensemble $| \mathscr{A} |$

(1) $a_1Rb_1, \ldots, a_mRb_m$

implique

(2) $f_{\mathscr{A}}(a_1, \ldots, a_m) R f_{\mathscr{A}}(b_1, \ldots, b_m)$,

où m est le rang de l'opération $f_{\mathscr{A}}$.

Soient $\mathscr{A} = \langle A, \Omega \rangle$ une algèbre, R une congruence dans $\mathscr{A}$ et A/R un ensemble quotient de l'ensemble A en R. Définissons sur l'ensemble A/R une opération m-aire $f_{\mathscr{A}/R}$ correspondant à l'opéra-

tion $f_{\mathcal{A}}$ de Ω de la façon suivante:

(3) $f_{\mathcal{A}/R}(a_1/R, \ldots, a_m/R) = f_{\mathcal{A}}(a_1, \ldots, a_m)/R$

pour tous $a_1, \ldots, a_m$ de A.

La définition est correcte, car, en vertu de (2), la valeur du second membre de (3) est indépendante du choix des éléments $a_1, \ldots, a_m$ respectivement dans les classes d'équivalence $a_1/R, \ldots, a_m/R$ (voir démonstration du théorème 1.9). L'opération $f_{\mathcal{A}/R}$ est appelée *opération associée à l'opération* $f_{\mathcal{A}}$ par la congruence R. Notons Ω^* l'ensemble de toutes les opérations associées aux opérations principales de l'algèbre $\mathcal{A}$ par congruence R, $\Omega^* = \{f_{\mathcal{A}/R} \mid f_{\mathcal{A}} \in \Omega\}$.

DÉFINITION. Soient $\mathcal{A} = \langle A, \Omega\rangle$ une algèbre et R une congruence dans $\mathcal{A}$. L'algèbre $\langle A/R, \Omega^*\rangle$ est dénommée *algèbre quotient* de l'algèbre $\mathcal{A}$ en congruence R et est notée $\mathcal{A}/R$.

THÉORÈME 2.11. *Soit R une congruence dans l'algèbre $\mathcal{A}$. L'application h de l'ensemble $\mid \mathcal{A} \mid$ dans $\mid \mathcal{A} \mid/R$ est alors telle que*

(1) $h(a) = a/R$ *pour tout* a *de* $\mid \mathcal{A} \mid$

est un homomorphisme de l'algèbre $\mathcal{A}$ sur l'algèbre quotient $\mathcal{A}/R$.

Démonstration. Il s'ensuit de (1) que h est une application de $\mid \mathcal{A} \mid$ sur $\mid \mathcal{A} \mid/R$. Il est nécessaire de montrer que h respecte toutes les opérations principales de l'algèbre $\mathcal{A}$. Soient $f_{\mathcal{A}}$ une opération principale quelconque de l'algèbre $\mathcal{A}$ et $f_{\mathcal{A}/R}$ l'opération principale associée de l'algèbre quotient $\mathcal{A}/R$. Alors, en vertu de (1), pour tous $a_1, \ldots, a_m$ de $\mid \mathcal{A} \mid$, on a

$$h(f_{\mathcal{A}}(a_1, \ldots, a_m)) = f_{\mathcal{A}}(a_1, \ldots, a_m)/R =$$
$$= f_{\mathcal{A}/R}(a_1/R, \ldots, a_m/R) =$$
$$= f_{\mathcal{A}/R}(h(a_1), \ldots, h(a_m)),$$

où m est le rang de l'opération $f_{\mathcal{A}}$. Par conséquent, h est un homomorphisme de l'algèbre $\mathcal{A}$ sur l'algèbre quotient $\mathcal{A}/R$. □

Notons que l'homomorphisme h défini à l'aide de (1) est appelé *homomorphisme naturel* de l'algèbre $\mathcal{A}$ sur l'algèbre quotient $\mathcal{A}/R$.

THÉORÈME 2.12. *Soient h un homomorphisme de l'algèbre $\mathcal{A}$ dans l'algèbre $\mathcal{B}$ et R une telle relation binaire sur $\mid \mathcal{A} \mid$ que pour tous a, b de $\mid \mathcal{A} \mid$, on ait*

(1) aRb *si et seulement si* $h(a) = h(b)$.

Dans ce cas R est une congruence dans l'algèbre $\mathcal{A}$.

Démonstration. La relation R est une équivalence d'application h et, en vertu du théorème 2.4.4, c'est une relation d'équivalence sur $\mid \mathcal{A} \mid$.

Soient $f_{\mathcal{A}}$ une opération principale quelconque (de rang m) de l'algèbre $\mathcal{A}$ et $f_{\mathcal{B}}$ l'opération principale correspondante de l'algèbre

$\mathscr{B}$. En vertu de (1), pour tous a_1, b_1, ..., a_m, b_m de l'ensemble $|\mathscr{A}|$ de

(2) $a_1Rb_1, \ldots, a_mRb_m$

s'ensuivent les égalités

(3) $h(a_1) = h(b_1), \ldots, h(a_m) = h(b_m)$.

Supposons que les éléments a_1, b_1, ..., a_m, b_m vérifient les conditions (2) et, partant, les conditions (3). Alors, puisque h est un homomorphisme de $\mathscr{A}$ dans $\mathscr{B}$, on a

$$\begin{aligned} h(f_{\mathscr{A}}(a_1, \ldots, a_m)) &= f_{\mathscr{B}}(h(a_1), \ldots, h(a_m)) = \\ &= f_{\mathscr{B}}(h(b_1), \ldots, h(b_m)) = \\ &= h(f_{\mathscr{A}}(b_1, \ldots, b_m)). \end{aligned}$$

Donc de (2) s'ensuit l'égalité

$$h(f_{\mathscr{A}}(a_1, \ldots, a_m)) = h(f_{\mathscr{A}}(b_1, \ldots, b_m)).$$

De là, par définition de R, il vient

(4) $f_{\mathscr{A}}(a_1, \ldots, a_m)\, Rf_{\mathscr{A}}(b_1, \ldots, b_m)$.

Bref, pour tous éléments a_1, b_1, ..., a_m, b_m de l'ensemble $|\mathscr{A}|$ de (2) s'ensuit (4). Par conséquent, R est une congruence dans $\mathscr{A}$. □

Exercices

1. Soient $+$, $\cdot$ des opérations banales d'addition et de multiplication sur l'ensemble **N** des nombres naturels et h l'application de l'ensemble **N** dans **N** telle que $h(x) = 2^x$ pour tout x de **N**. Démontrer que h est un homomorphisme de l'algèbre $\langle \mathbf{N}, + \rangle$ dans l'algèbre $\langle \mathbf{N}, \cdot \rangle$.

2. Soient $+$ et $\cdot$ des opérations banales d'addition et de multiplication sur l'ensemble **R** des nombres réels et a un nombre réel positif fixé. Soit h l'application de **R** dans **R** telle que $h(x) = a^x$ pour tout x de **R**. Démontrer que h est un homomorphisme de l'algèbre $\langle \mathbf{R}, + \rangle$ dans l'algèbre $\langle \mathbf{R}, \cdot \rangle$.

3. Soit h un homomorphisme de l'algèbre $\langle A, f \rangle$ sur 'algèbre $\langle B, g \rangle$, où f et g sont des opérations binaires. Démontrer que:

(a) si l'opération f est commutative, l'opération g l'est également;

(b) si l'opération f est associative, l'opération g l'est également;

(c) si e est un élément neutre relativement à l'opération f, $f(e)$ est un élément neutre relativement à l'opération g;

(d) si l'élément x est symétrisable relativement à l'opération f, l'élément $f(x)$ est symétrisable relativement à l'opération g; si les éléments x et x' sont mutuellement symétriques relativement à l'opération f, les éléments $f(x)$ et $f(x')$ sont alors mutuellement symétriques relativement à l'opération g.

4. Soient **N** un ensemble des nombres naturels et $B = \{2^x \mid x \in \mathbf{N}\}$. Soit h l'application de l'algèbre $\langle \mathbf{N}, + \rangle$ sur l'algèbre $\langle B, \cdot \rangle$ telle que pour tout x de **N** se vérifie l'égalité $h(x) = 2^x$. Montrer que h est un isomorphisme.

5. Soient **R** un ensemble des nombres réels, $\mathbf{R}_+^*$ un ensemble des nombres réels positifs, a un nombre réel positif autre que un. Soit h l'application de l'algèbre $\langle \mathbf{R}, + \rangle$ dans l'algèbre $\langle \mathbf{R}_+^*, \cdot \rangle$ telle que $h(x) = a^x$ pour chaque x de **R**. Démontrer que h est un isomorphisme.

6. Soient f un monomorphisme de l'algèbre $\mathcal{A}$ dans $\mathcal{B}$ et g un monomorphisme de l'algèbre $\mathcal{B}$ dans l'algèbre $\mathcal{C}$. Démontrer que la composition $g \circ f$ est un monomorphisme de l'algèbre $\mathcal{A}$ dans l'algèbre $\mathcal{C}$.

7. Fournir un exemple d'algèbre $\mathcal{A}$ et de relation d'équivalence R sur $|\mathcal{A}|$ qui ne soit pas une congruence dans l'algèbre $\mathcal{A}$.

8. Soit h un homomorphisme de l'algèbre $\mathcal{A}$ dans l'algèbre $\mathcal{B}$. Démontrer que l'ensemble Im $|\mathcal{A}|$ (image homomorphe de l'ensemble de base de l'algèbre $\mathcal{A}$) est clos dans l'algèbre $\mathcal{B}$.

9. Soit h un homomorphisme de l'algèbre $\mathcal{A}$ dans l'algèbre $\mathcal{B}$. Démontrer que l'algèbre

$$\langle \mathcal{C}, f_1 \mid \mathcal{C}, \ldots, f_s \mid \mathcal{C} \rangle,$$

où $\mathcal{C} = \text{Im}\,|\mathcal{A}|$, est une sous-algèbre de l'algèbre $\mathcal{B} = \langle \mathcal{B}, f_1, \ldots, f_s \rangle$. Cette algèbre est appelée *image homomorphe* de l'algèbre $\mathcal{A}$ avec homomorphisme h.

10. Soit h un homomorphisme de l'algèbre $\mathcal{A}$ dans l'algèbre $\mathcal{B}$. Démontrer que l'image homomorphe de l'algèbre $\mathcal{A}$ avec cet homomorphisme est isomorphe à l'algèbre quotient $\mathcal{A}/R$, où R est une congruence engendrée par l'homomorphisme h.

11. Démontrer que tout homomorphisme h de l'algèbre $\mathcal{A}$ sur l'algèbre $\mathcal{B}$ est une composition de l'homomorphisme naturel de l'algèbre $\mathcal{A}$ sur son algèbre quotient et de l'isomorphisme de cette algèbre quotient sur l'algèbre $\mathcal{B}$.

§ 3. Groupes

Notion de groupe. Cette notion est un cas particulier d'algèbres qui joue un rôle important en mathématiques théoriques et appliquées.

DÉFINITION. L'algèbre $\mathcal{G} = \langle G, *, ' \rangle$ du type (2, 1) est appelée *groupe* si ses opérations principales vérifient les conditions (axiomes):

(1) l'opération binaire $*$ est associative, c'est-à-dire pour tous éléments a, b, c de G $a * (b * c) = (a * b) * c$;

(2) il y a dans G un élément neutre à droite relativement à l'opération $*$, c'est-à-dire un tel élément e pour lequel $a * e = a$ quel que soit a de G;

(3) pour tout élément a de G on a l'égalité $a * a' = e$.

Ainsi, le groupe est un ensemble non vide muni de deux opérations: une opération binaire $*$ et une opération singulaire $'$. L'opération binaire est associative et comporte un élément neutre à droite, tandis que l'opération singulaire est une opération de passage à l'élément symétrique à droite relativement à l'opération binaire et, par suite, chaque élément du groupe comporte un élément symétrique à droite relativement à l'opération binaire du groupe $*$.

DÉFINITION. Un groupe $\mathcal{G} = \langle G, *, ' \rangle$ est dit *abélien* ou *commutatif* si l'opération binaire du groupe $*$ est commutative, c'est-à-dire si pour tous a, b de G $a * b = b * a$.

DÉFINITION. On appelle *ordre du groupe* $\mathcal{G} = \langle G, *, ' \rangle$ le nombre d'éléments de l'ensemble de base G du groupe lorsque G est fini. Si G

est un ensemble infini, le groupe $\mathscr{G}$ est dénommé *groupe d'ordre infini.*

En étudiant les groupes on utilise habituellement pour les opérations principales du groupe des notations additive ou multiplicative. Avec l'utilisation de la *notation multiplicative* l'opération binaire du groupe est appelée *multiplication* et l'on écrit $a \cdot b$ (ou ab) au lieu de $a * b$ en appelant l'élément $a \cdot b$ *produit des éléments* a et b. L'élément symétrique de a noté a^{-1} est appelé *inverse de l'élément* a. L'élément neutre par rapport à la multiplication est noté e, 1 ou $1_{\mathscr{G}}$ et on l'appelle *élément unitaire* ou *unité du groupe.* Dans la notation multiplicative la définition susmentionnée du groupe s'énonce de la façon suivante.

L'algèbre $\mathscr{G} = \langle G, \cdot, ^{-1} \rangle$ du type (2, 1) est appelée *groupe* si ses opérations principales vérifient les conditions:

(1) l'opération binaire $\cdot$ est associative, c'est-à-dire pour tous éléments a, b, c de G se vérifie l'égalité $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

(2) il y a dans G une unité droite, c'est-à-dire un élément e tel que $a \cdot e = a$ pour tout élément a de G;

(3) pour tout élément a de G on a l'égalité $a \cdot a^{-1} = e$.

La notion de puissance naturelle a^n de l'élément a d'un groupe multiplicatif $\langle G, \cdot, ^{-1} \rangle$ se définit de la façon suivante:

$$a^0 = e, \quad a^n = a \cdot a \ldots a \text{ pour } n \in \mathbf{N} \setminus \{0\}.$$

Dans une *notation additive* l'opération binaire du groupe est appelée *addition* et l'on écrit $a + b$ au lieu de $a * b$ en appelant l'élément $a + b$ *somme des éléments* a et b. L'élément symétrique de l'élément a est noté $(-a)$ et s'appelle *élément opposé de* a. L'élément neutre par rapport à l'addition est désigné par le symbole 0 ou $0_{\mathscr{G}}$ et est appelé *élément zéro* ou *zéro du groupe.* En écriture additive la définition du groupe est formulée de la façon suivante.

L'algèbre $\mathscr{G} = \langle G, +, - \rangle$ du type (2, 1) est dénommée *groupe* si ses opérations principales vérifient les conditions:

(1) l'opération binaire $+$ est associative, c'est-à-dire que pour tous éléments a, b, c de G on a $a + (b + c) = (a + b) + c$;

(2) il y a dans G un zéro à droite, c'est-à-dire un élément 0 tel que $a + 0 = a$ pour tout élément a de G;

(3) pour tout élément a de G $a + (-a) = 0$.

Exemples de groupes. 1. Soit Q l'ensemble de tous les nombres rationnels avec une addition banale et une opération singulaire $-$, opération de passage du nombre a au nombre opposé $(-a)$. L'algèbre $\mathscr{Q} = \langle \mathbf{Q}, +, - \rangle$ du type (2, 1) est un groupe. Il est dit *groupe additif des nombres rationnels.*

2. Soit $\mathbf{Q}^*$ l'ensemble de tous les nombres rationnels autres que zéro avec multiplication banale et opération singulaire $^{-1}$, opération de passage du nombre a au nombre inverse a^{-1}. L'algèbre

$\mathscr{Q}^* = \langle \mathbf{Q}^*, \cdot, {}^{-1} \rangle$ est un groupe. Ce groupe est appelé *groupe multiplicatif des nombres rationnels.*

3. Soient **R** l'ensemble de tous les nombres réels avec addition banale et opération singulaire associant à chaque nombre réel r le nombre opposé $-r$. L'algèbre $\mathscr{R}_+ = \langle \mathbf{R}, +, - \rangle$ est un groupe. Il s'appelle *groupe additif des nombres réels.*

4. Soient $\mathbf{R}^*$ l'ensemble de tous les nombres réels autres que zéro avec multiplication banale et opération singulaire ${}^{-1}$ qui associe à chaque nombre r différent de zéro son inverse r^{-1}. L'algèbre $\mathscr{R}^* = \langle \mathbf{R}^*, \cdot, {}^{-1} \rangle$ est un groupe. Ce groupe est appelé *groupe multiplicatif des nombres réels.*

5. Soit S_n une collection de toutes les permutations de l'ensemble $M = \{1, \ldots, n\}$, c'est-à-dire une collection d'applications injectives de cet ensemble sur lui-même. Soient $\mathscr{S}_n = \langle S_n, \circ, {}^{-1} \rangle$ une algèbre avec une opération binaire $\circ$ (composition d'applications) et une opération singulaire ${}^{-1}$ associant la fonction f de S_n à sa fonction inverse f^{-1}. Cette algèbre est un groupe. En effet, suivant le théorème 2.3.10 une composition de deux permutations quelconques de l'ensemble M est une permutation de cet ensemble. Selon le théorème 2.3.5 une composition de permutations est associative. Une permutation identique i_M est un élément neutre relativement à une composition de permutations. Pour toute permutation f de l'ensemble M $f \circ f^{-1} = i_M$. Ce groupe est dénommé *groupe symétrique des permutations d'indice n*; il possède l'ordre $n!$ et n'est pas commutatif pour $n > 2$.

6. Soit G l'ensemble de tous les vecteurs d'un plan donné avec l'opération banale $+$ d'addition des vecteurs et l'opération singulaire $-$ associant chaque vecteur v à son opposé $(-v)$. L'algèbre $\langle G, +, - \rangle$ est un groupe. Ce groupe est appelé *groupe additif des vecteurs du plan.*

7. Considérons l'ensemble G de toutes les rotations du plan autour d'un point donné O. Une rotation du plan est assimilée à une transformation du plan, c'est-à-dire à une application injective du plan sur lui-même. Deux rotations d'angles α et β sont dites coïncidentes si $\alpha - \beta = 2n\pi$, où n est un entier. La composition $\varphi \circ \psi$ de deux rotations ψ et φ respectivement d'angles α et β est une rotation d'angle $\alpha + \beta$. Si ψ est une rotation d'angle α, ψ^{-1} est une rotation d'angle $(-\alpha)$. L'algèbre $\langle G, \circ, {}^{-1} \rangle$ est un groupe. Il est dénommé *groupe de rotations du plan* autour du point donné.

8. Soit H_n un ensemble composé de n rotations d'un plan donné d'angles $2k\pi/n$, $k = 0, 1, \ldots, n-1$, autour d'un point O fixe, constituant une application d'un polygone régulier à n angles de centre au point O sur lui-même. L'algèbre $\langle H_n, \circ, {}^{-1} \rangle$ est un groupe. Il est appelé *groupe de rotation d'un polygone régulier à n angles.*

9. Considérons un ensemble G de toutes les rotations d'un espace autour du point O, constituant une application d'un corps régulier

donné (tétraèdre, cube, icosaèdre, dodécaèdre) de centre au point O sur lui même. L'algèbre $\langle G, \circ, {}^{-1}\rangle$ est un groupe. Il est appelé *groupe de rotations* (*autocoïncidences*) *du corps régulier donné.*

Propriétés élémentaires du groupe. On utilisera plus loin la notation multiplicative pour les opérations du groupe.

PROPRIÉTÉ 3.1. *Pour tout élément a du groupe $a^{-1}a = e$, c'est-à-dire l'inverse à droite de a est également un inverse à gauche.*

Démonstration. Du deuxième et du troisième axiomes du groupe il s'ensuit que

$$a^{-1} = a^{-1}e = a^{-1}(aa^{-1}) = (a^{-1}a)\, a^{-1}.$$

En vertu des axiomes du groupe on en déduit les égalités

$$a^{-1}a = (a^{-1}a)\, e = (a^{-1}a)\,(a^{-1}(a^{-1})^{-1}) = ((a^{-1}a)\, a^{-1})\,(a^{-1})^{-1} =$$
$$= a^{-1}(a^{-1})^{-1} = e, \text{ c'est-à-dire } a^{-1}a = e. \quad \square$$

PROPRIÉTÉ 3.2. *Pour chaque élément a du groupe l'élément a^{-1} est l'unique élément inverse. Chaque élément a du groupe possède un élément inverse unique à droite et un élément inverse unique à gauche, les deux coïncidant avec a^{-1}.*

Cette propriété découle directement de la définition de l'élément inverse, de la propriété 3.1, du théorème 1.4 et du corollaire 1.5 de ce dernier.

PROPRIÉTÉ 3.3. *Pour tout élément a du groupe $ea = a$, c'est-à-dire que l'unité droite est également une unité gauche.*

Démonstration. A partir des axiomes du groupe et de la propriété 3.1. il s'ensuit que

$$ea = (aa^{-1})\, a = a\,(a^{-1}a) = ae = a, \text{ c'est-à-dire } ea = a. \quad \square$$

PROPRIÉTÉ 3.4. *L'élément e du groupe est l'unique élément unité du groupe. C'est également l'unique élément unité droite et unité gauche du groupe.*

Cette propriété découle directement de la définition des éléments unités, de la propriété 3.3, du théorème 1.1 et du corollaire 1.2 de ce dernier.

PROPRIÉTÉ 3.5. *Pour tous éléments a, b du groupe chacune des équations $ax = b$ et $ya = b$ relativement aux variables x et y possède dans le groupe une solution unique.*

Démonstration. L'élément $a^{-1}b$ est la solution de l'équation $ax = b$, car $a(a^{-1}b) = (aa^{-1})\, b = eb = b$. D'autre part, si c est une solution arbitraire de l'équation $ax = b$, on a $c = ec = (a^{-1}a)\, c = a^{-1}(ac) = a^{-1}b$. Par conséquent, l'élément $a^{-1}b$ est l'unique solution de la première équation. On démontre de façon analogue que l'élément ba^{-1} est l'unique solution de la seconde équation. $\square$

PROPRIÉTÉ 3.6 (*règle de simplification*). *Pour tous éléments a, b, c du groupe de $ac = bc$ s'ensuit $a = b$ et de $ca = cb$ $a = b$.*

Démonstration. Si $ac = bc$, a et b sont les solutions de l'équation $yc = bc$. De la propriété 3.3 on déduit que $a = b$. On démontre de façon analogue que de $ca = cb$ s'ensuit $a = b$. □

PROPRIÉTÉ 3.7. *Pour tous éléments a, b, c du groupe il s'ensuit de $ab = a$ que $b = e$ et de $ca = a$ que $c = e$.*

Démonstration. Si $ab = a$, on a $ab = ae$. Selon la règle de simplification de $ab = ae$ s'ensuit $b = e$. De façon analogue de $ca = a$ on déduit que $ca = ea$ et $c = e$. □

PROPRIÉTÉ 3.8. *L'élément a est dans le groupe l'inverse de a^{-1}, c'est-à-dire que $(a^{-1})^{-1} = a$.*

Démonstration. D'après le troisième axiome du groupe $(a^{-1})(a^{-1})^{-1} = e$. Selon la propriété 3.1 $a^{-1}a = e$. Donc, $a^{-1}(a^{-1})^{-1} = a^{-1}a$. Selon la règle de simplification il s'ensuit l'égalité $(a^{-1})^{-1} = a$. □

PROPRIÉTÉ 3.9. *Pour tous éléments a, b du groupe de $ab = e$ s'ensuit $b = a^{-1}$ et $a = b^{-1}$.*

Cette propriété découle directement de la définition de l'élément inverse et de la propriété 3.2.

Homomorphismes des groupes. En accord avec la définition de l'homomorphisme des algèbres ainsi qu'avec le fait que les groupes sont un cas particulier des algèbres formulons les définitions suivantes.

Soient $\mathcal{G} = \langle G, \cdot, ^{-1}\rangle$ et $\mathcal{H} = \langle H, \circ, ^{-1}\rangle$ des groupes multiplicatifs.

On dit que l'application h de l'ensemble G dans H respecte les opérations principales du groupe $\mathcal{G}$ si sont satisfaites les conditions:

(1) $h(ab) = h(a) \circ h(b)$ pour tous a, b de G;

(2) $h(a^{-1}) = (h(a))^{-1}$ pour tout a de G.

DÉFINITION. On appelle *homomorphisme du groupe $\mathcal{G}$* dans (sur) le groupe $\mathcal{H}$ toute application de l'ensemble G dans (sur) H respectant les opérations principales du groupe $\mathcal{G}$. L'homomorphisme du groupe $\mathcal{G}$ sur $\mathcal{H}$ est appelé *épimorphisme*.

DÉFINITION. On appelle *isomorphisme* tout homomorphisme h du groupe $\mathcal{G}$ sur le groupe $\mathcal{H}$ si h est une application injective de l'ensemble G sur H. Les groupes $\mathcal{G}$ et $\mathcal{H}$ sont dits *isomorphes* s'il y a isomorphisme du groupe $\mathcal{G}$ sur $\mathcal{H}$.

La notation $\mathcal{G} \cong \mathcal{H}$ signifie que les groupes $\mathcal{G}$ et $\mathcal{H}$ sont isomorphes.

DÉFINITION. On appelle *monomorphisme* ou *injection* l'homomorphisme h du groupe $\mathcal{G}$ dans le groupe $\mathcal{H}$ si h est une application injective de l'ensemble G dans H.

DÉFINITION. On appelle *endomorphisme du groupe* $\mathcal{G}$ l'homomorphisme de $\mathcal{G}$ dans lui-même. L'isomorphisme de $\mathcal{G}$ sur lui-même est appelé *automorphisme du groupe* $\mathcal{G}$.

Ainsi, par exemple, est un automorphisme une application identique du groupe sur lui-même.

THÉORÈME 3.1. *Si l'application h du groupe* $\mathcal{G} = \langle G, \cdot, ^{-1}\rangle$ *dans le groupe* $\mathcal{H} = \langle H, \circ, ^{-1}\rangle$ *respecte l'opération binaire du groupe* $\mathcal{G}$, *c'est-à-dire si*

(1) $h(ab) = h(a) \circ h(b)$ *pour tous* a, b *de* G,

alors h transforme l'unité du groupe $\mathcal{G}$ *en l'unité du groupe* $\mathcal{H}$ *et constitue un homomorphisme.*

D é m o n s t r a t i o n. Soient e l'unité du groupe $\mathcal{G}$ et $e' = h(e)$. En vertu de (1), $h(e \cdot e) = h(e) \circ h(e) = h(e)$, c'est-à-dire que $e' \circ e' = e'$. De là, en raison de la propriété 3.7, il s'ensuit que e' est une unité du groupe $\mathcal{H}$.

Soit a un élément quelconque du groupe $\mathcal{G}$. En vertu de (1), de $a \cdot a^{-1} = e$ s'ensuit $h(a) \circ h(a^{-1}) = e'$. Selon la propriété 3.9 on obtient

(2) $h(a^{-1}) = (h(a))^{-1}$ pour tout a de G.

Sur la base de (1) et (2) on conclut que h est un homomorphisme du groupe $\mathcal{G}$ dans $\mathcal{H}$. □

THÉORÈME 3.2. *Sur un ensemble de groupes quelconque la relation d'isomorphisme est réflexive, transitive et symétrique, c'est-à-dire est une relation d'équivalence.*

Ce théorème découle directement du théorème 2.5.

E x e m p l e s. 1. Considérons un ensemble $\mathbf{Q}^*$ de tous les nombres rationnels autres que zéro et $\mathcal{Q}^* = \langle \mathbf{Q}^*, \cdot, ^{-1}\rangle$ constituant un groupe multiplicatif des nombres rationnels. Soient $\mathbf{Q}_+$ l'ensemble de tous les nombres rationnels positifs et $\mathcal{Q}_+ = \langle \mathbf{Q}_+, \cdot, ^{-1}\rangle$ un groupe multiplicatif des nombres rationnels positifs. L'application h de l'ensemble $\mathbf{Q}^*$ sur $\mathbf{Q}_+$ définie par la formule $h(a) = |a|$ pour chaque a de $\mathbf{Q}^*$, où $|a|$ est la valeur absolue du nombre a, respecte les opérations principales du groupe $\mathcal{Q}^*$. En effet, pour tous a, b de $\mathbf{Q}^*$ se vérifient les égalités $|ab| = |a||b|$ et $|a^{-1}| = |a|^{-1}$. Par conséquent, l'application h est un homomorphisme du groupe $\mathcal{Q}^*$ sur $\mathcal{Q}_+$.

2. Considérons un ensemble $\mathbf{R}_+$ de tous les nombres réels positifs et $\mathcal{R}_+ = \langle \mathbf{R}_+, \cdot, ^{-1}\rangle$ constituant un groupe multiplicatif des nombres réels positifs. Soient $\mathbf{R}$ l'ensemble de tous les nombres réels et $\mathcal{R} = \langle \mathbf{R}, +, -\rangle$ le groupe additif des nombres réels. Voyons l'application $f: \mathbf{R}_+ \to \mathbf{R}$ définie par la formule $f(x) = \log x$. La fonction f est une application injective de l'ensemble $\mathbf{R}_+$ sur $\mathbf{R}$ qui respecte les opérations principales du groupe $\mathcal{R}_+$. En effet, pour tous x, y de $\mathbf{R}_+$

$$\log(xy) = \log x + \log y, \quad \log(x^{-1}) = -\log x.$$

Par conséquent, f est un isomorphisme du groupe $\mathcal{R}_+$ sur le groupe $\mathcal{R}$.

3. Considérons l'application g de l'ensemble **R** sur $\mathbf{R}_+$ définie par la formule $g(x) = 2^x$. L'application g est une application injective de **R** sur $\mathbf{R}_+$ et elle respecte les opérations principales du groupe additif $\mathcal{R} = \langle \mathbf{R}, +, - \rangle$, car $2^{x+y} = 2^x 2^y$ et $2^{-x} = (2^x)^{-1}$. Donc, g est un isomorphisme du groupe additif $\mathcal{R}$ sur le groupe multiplicatif $\mathcal{R}_+ = \langle \mathbf{R}, \cdot, ^{-1} \rangle$.

Sous-groupes. Considérons le groupe $\mathcal{G} = \langle G, \cdot, ^{-1} \rangle$.

DÉFINITION. On appelle *sous-groupe du groupe* $\mathcal{G}$ toute sous-algèbre de ce groupe.

De manière plus détaillée, en fonction de la définition de la sous-algèbre, la définition du sous-groupe peut être énoncée de la façon suivante.

L'algèbre $\mathcal{H} = \langle H, \odot, ^{-1} \rangle$ du type (2, 1) est appelée *sous-groupe du groupe* $\mathcal{G} = \langle G, \cdot, ^{-1} \rangle$ si $H \subset G$ et si l'application identique de l'ensemble H dans G est un monomorphisme de l'algèbre $\mathcal{H}$ dans $\mathcal{G}$, c'est-à-dire si sont satisfaites les conditions:

(1) $a \odot b = a \cdot b$ pour tous a, b de H;

(2) $a^{-1} = a^{-1}$ pour tout a de H.

La notation $\mathcal{H} \dashv \mathcal{G}$ signifie que l'algèbre $\mathcal{H}$ est un sous-groupe du groupe $\mathcal{G}$.

Si $\mathcal{H} \dashv \mathcal{G}$, alors de la définition du sous-groupe il s'ensuit que l'ensemble H est clos dans le groupe $\mathcal{G}$ et, par suite, l'application de toute opération principale du groupe $\mathcal{G}$ aux éléments de H aboutit de nouveau à l'élément de H. En outre, en vertu des conditions (1) et (2) chacune des opérations principales de l'algèbre $\mathcal{H}$ est une restriction de l'opération principale correspondante du groupe $\mathcal{G}$ à l'ensemble H.

THÉORÈME 3.3. *Tout sous-groupe du groupe est un groupe. L'élément neutre du groupe est l'élément neutre de son sous-groupe quelconque.*

Démonstration. Soient $\mathcal{H} = \langle H, \odot, ^{-1} \rangle$ un sous-groupe du groupe multiplicatif $\mathcal{G} = \langle G, \cdot, ^{-1} \rangle$ et e l'élément neutre du groupe $\mathcal{G}$.

L'opération binaire $\odot$ de l'algèbre $\mathcal{H}$ est associative, car, en vertu de (1), pour tous a, b, c de H, on a

$$a \odot (b \odot c) = a \cdot (b \cdot c) = (a \cdot b) \cdot c = (a \odot b) \odot c.$$

L'élément e appartient à H, car, en vertu de (1) et (2), pour tout a de H, on a $e = a \cdot a^{-1} = a \odot a^{-1} \in H$. En vertu de (1), pour tout a de H se vérifient les égalités $a \odot e = a \cdot e = a$, c'est-à-dire que e est un élément neutre à droite relativement à l'opération $\odot$.

En vertu de (2), pour tout a de H on obtient $a \odot a^{-1} = a \cdot a^{-1} = e$, c'est-à-dire que $a \odot a^{-1} = e$. Par conséquent, l'algèbre $\mathcal{H}$ est un groupe et e est son élément neutre. □

Soient $\mathscr{G} = \langle G, \cdot, ^{-1} \rangle$ un groupe multiplicatif et A un sous-ensemble non vide de l'ensemble G fermé relativement aux opérations principales du groupe $\mathscr{G}$. Soient $\odot$ et $^{-1}$ les restrictions des opérations principales du groupe $\mathscr{G}$ à l'ensemble A, autrement dit

$a \odot b = a \cdot b$ pour tous a, b de A;

$a^{-1} = a^{-1}$ pour tout a de A.

Alors, suivant le théorème 2.6 et 3.3 l'algèbre

(3) $\mathscr{A} = \langle A, \odot, ^{-1} \rangle$

est un sous-groupe du groupe $\mathscr{G}$. Donc, le sous-groupe $\mathscr{A}$ du groupe $\mathscr{G}$ est défini de façon univoque par le sous-ensemble non vide A clos dans $\mathscr{G}$. Aussi au lieu de la notation (3) écrit-on: « sous-groupe $\mathscr{A} = \langle A, \cdot, ^{-1} \rangle$ » et lit-on: « l'ensemble A est un sous-groupe du groupe $\mathscr{G}$ par rapport aux opérations $\cdot$ et $^{-1}$ ».

THÉORÈME 3.4. *La relation binaire* $\dashv$ (« *appartenir à un sous-groupe* ») *sur l'ensemble des sous-groupes du groupe donné est réflexive, transitive et antisymétrique et, partant, c'est une relation d'ordre non strict.*

Ce théorème est un cas particulier du théorème 2.8.

THÉORÈME 3.5. *Une intersection d'une collection arbitraire (non vide) de sous-groupes du groupe* $\mathscr{G}$ *est un sous-groupe du groupe* $\mathscr{G}$.

Ce théorème découle directement du théorème 3.3.

Il s'ensuit du théorème 3.6 que pour tout ensemble M d'éléments du groupe $\mathscr{G}$ il existe un sous-groupe minimal $\mathscr{H}$ contenant M. Il est facile de voir que $\mathscr{H}$ est une intersection de tous les sous-groupes du groupe $\mathscr{G}$ contenant M. Ce sous-groupe minimal $\mathscr{H}$ est dénommé *sous-groupe engendré par l'ensemble* M, tandis que M est appelé *ensemble de génératrices* ou *système de génératrices du groupe* $\mathscr{H}$.

DÉFINITION. Un groupe est dit *cyclique* s'il est engendré par un seul élément (ensemble à un élément).

Exemples. 1. Considérons un groupe additif $\mathscr{R}_+ = \langle \mathbf{R}, +, - \rangle$ des nombres réels. L'ensemble $\mathbf{Q}$ des nombres rationnels est un sous-ensemble de l'ensemble $\mathbf{R}$ qui est fermé aux opérations principales du groupe $\mathscr{R}_+$. Donc, l'algèbre $\mathscr{Q} = \langle \mathbf{Q}, +, - \rangle$, groupe additif des nombres rationnels, est un sous-groupe du groupe $\mathscr{R}_+$.

2. Considérons un groupe multiplicatif $\mathscr{R}^* = \langle \mathbf{R}^*, \cdot, ^{-1} \rangle$ des nombres réels. L'ensemble $\mathbf{Q}^*$ des nombres rationnels différents de zéro est un sous-ensemble de l'ensemble $\mathbf{R}^*$ fermé aux opérations principales du groupe $\mathscr{R}^*$. Donc, l'algèbre $\mathscr{Q}^* = \langle \mathbf{Q}^*, \cdot, ^{-1} \rangle$, groupe multiplicatif des nombres rationnels, est un sous-groupe du groupe $\mathscr{R}^*$.

3. Soient $\mathscr{G} = \langle G, \cdot, ^{-1} \rangle$ un groupe de rotations du plan autour du point donné O et H_n un ensemble composé de n rotations du plan autour du point O constituant une application d'un polygone régu-

lier à n angles de centre O sur lui-même. L'ensemble H_n est clos par rapport aux opérations principales du groupe $\mathcal{G}$. Donc, l'algèbre $\mathcal{H}_n = \langle H_n, \circ, ^{-1}\rangle$, groupe de rotations d'un polygone régulier à n angles, est un sous-groupe du groupe $\mathcal{G}$.

Exercices

1. Elucider si les ensembles des nombres rationnels suivants sont clos relativement aux opérations principales du groupe additif des nombres rationnels:
(a) l'ensemble de tous les entiers;
(b) l'ensemble de tous les nombres naturels;
(c) l'ensemble de tous les entiers pairs;
(d) l'ensemble de tous les entiers multiples de l'entier donné n;
(e) l'ensemble de tous les entiers impairs;
(f) l'ensemble de tous les nombres rationnels à dénominateurs impairs;
(g) l'ensemble de tous les nombres rationnels à dénominateurs pairs.

2. Elucider si les ensembles des nombres rationnels suivants sont clos par rapport aux opérations principales du groupe multiplicatif des nombres rationnels:
(a) l'ensemble $\{1, -1\}$;
(b) l'ensemble de tous les nombres autres que zéro à dénominateurs pairs;
(c) l'ensemble de tous les nombres rationnels autres que zéro à dénominateurs impairs;
(d) l'ensemble de toutes les puissances entières du nombre 2;
(e) l'ensemble $\{p^n \mid n \text{ entier}\}$, où p est un nombre premier.

3. Former la table de multiplication pour les éléments des groupes suivants:
(a) le groupe de rotations d'un triangle équilatéral;
(b) le groupe de rotations d'un carré;
(c) le groupe de rotations d'un pentagone régulier;
(d) le groupe additif des classes résiduelles modulo 5;
(e) le groupe multiplicatif des classes résiduelles modulo 5, constituant des nombres premiers avec 5;
(f) le groupe de toutes les symétries du losange;
(g) le groupe de toutes les symétries d'un triangle équilatéral;
(h) le groupe symétrique des permutations de troisième degré;
(i) le groupe des symétries d'un rectangle qui ne soit pas un carré;
(j) le groupe de toutes les symétries d'un carré.

4. Démontrer par récurrence que l'ordre du groupe symétrique des permutations de degré n et $n!$

5. Démontrer que si $a^2 = e$ (e étant l'élément unité du groupe) pour tout élément a du groupe multiplicatif, alors le groupe est abélien.

6. Soient g et h les éléments du groupe multiplicatif $\mathcal{G}$. Déterminons la puissance à exposant négatif: $a^{-n} = (a^{-1})^n$. Démontrer que pour tous nombres m et n:

(a) $(g^{-1})^n = (g^n)^{-1}$;
(b) $g^m g^n = g^{m+n}$;
(c) $(g^m)^n = g^{mn}$;
(d) $(g \cdot h)^m = g^m \cdot h^m$ si $\mathcal{G}$ est un groupe abélien.

7. Démontrer que tout groupe à quatre ou moins d'éléments est un groupe abélien.

8. Montrer que tout groupe à trois éléments est cyclique. Démontrer que tous deux groupes comportant trois éléments chacun sont isomorphes.

9. Soient $\mathcal{G}$ un groupe abélien additif et n un entier. Montrer que l'application $x \longmapsto nx$ est un endomorphisme du groupe $\mathcal{G}$.

10. Montrer que l'application $x \longmapsto 3^x$ est un isomorphisme du groupe additif des nombres réels sur un groupe multiplicatif des nombres réels positifs.

11. Démontrer que le groupe symétrique des permutations à trois éléments est isomorphe au groupe des symétries du triangle équilatéral.

12. Démontrer que le groupe des rotations du carré n'est pas isomorphe au groupe des symétries du losange.

13. Considérer un groupe abélien multiplicatif $\mathcal{G}$. Montrer que l'application $x \longmapsto x^{-1}$ est un automorphisme du groupe $\mathcal{G}$.

14. Démontrer que le groupe des symétries d'un tétraèdre régulier est isomorphe au groupe symétrique des permutations à quatre éléments.

15. Démontrer qu'une algèbre isomorphe au groupe est un groupe.

§ 4. Anneaux

Notion d'anneau. Les anneaux comme les groupes sont un cas particulier fort important des algèbres.

Définition. On appelle *anneau* une algèbre $\mathcal{K} = \langle K, +, -, \cdot, 1\rangle$ du type (2, 1, 2, 0) dont les opérations principales vérifient les conditions suivantes:

(1) l'algèbre $\langle K, +, -\rangle$ est un groupe abélien;

(2) l'algèbre $\langle K, \cdot, 1\rangle$ est un monoïde;

(3) la multiplication est distributive par rapport à l'addition, c'est-à-dire pour tous éléments a, b, c de K

$$(a + b)\cdot c = a\cdot c + b\cdot c, \quad c\cdot(a + b) = c\cdot a + c\cdot b.$$

L'ensemble de base K de l'anneau $\mathcal{K}$ est également noté $|\mathcal{K}|$. Les éléments de l'ensemble K sont appelés *éléments de l'anneau* $\mathcal{K}$.

Définition. Le groupe $\langle K, +, -\rangle$ est appelé *groupe additif de l'anneau* $\mathcal{K}$. Le zéro de ce groupe, c'est-à-dire l'élément neutre par rapport à l'addition, est dénommé *zéro de l'anneau* et est noté 0 ou $0_{\mathcal{K}}$.

Définition. Un monoïde $\langle K, \cdot, 1\rangle$ est appelé *monoïde multiplicatif de l'anneau* $\mathcal{K}$. L'élément 1 noté également $1_{\mathcal{K}}$ constituant un élément neutre par rapport à la multiplication est appelé *unité de l'anneau* $\mathcal{K}$.

L'anneau $\mathcal{K}$ est dit *commutatif* si $a\cdot b = b\cdot a$ pour tous éléments a, b de l'anneau. L'anneau $\mathcal{K}$ est dit *nul* si $|\mathcal{K}| = \{0_{\mathcal{K}}\}$.

Définition. Un anneau $\mathcal{K}$ est appelé *domaine d'intégrité* s'il est commutatif, $0_{\mathcal{K}} \neq 1_{\mathcal{K}}$ et pour tous a, $b \in K$ de $a\cdot b = 0$ s'ensuit $a = 0$ ou $b = 0$.

Définition. Les éléments a et b de l'anneau $\mathcal{K}$ sont appelés *diviseurs de zéro*, si $a \neq 0$, $b \neq 0$ et $ab = 0$ ou $ba = 0$.

Remarquons que tout domaine d'intégrité ne comporte pas de diviseurs de zéro.

E x e m p l e s. 1. Soit **Q** un ensemble de tous les nombres rationnels et

$$\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}.$$

L'algèbre

$$\mathfrak{A}[\sqrt{2}] = \langle \mathbf{Q}[\sqrt{2}], +, -, \cdot, 1 \rangle$$

du type (2, 1, 2, 0), où $+$, $\cdot$ sont des opérations banales d'addition et de multiplication des nombres réels et — une opération singulaire de passage du nombre donné à son opposé, est un anneau commutatif.

2. Considérons un ensemble K de toutes les fonctions réelles définies sur l'ensemble **R** des nombres réels. La somme $f + g$, le produit $f \cdot g$, la fonction $(-f)$ et la fonction unitaire **1** se définissent comme habituellement, à savoir:

$$(f + g)(x) = f(x) + g(x);$$
$$(f \cdot g)(x) = f(x) \cdot g(x);$$
$$(-f)(x) = -f(x);$$
$$\mathbf{1}(x) = 1.$$

Une vérification directe montre que l'algèbre $\langle K, +, -, \cdot, \mathbf{1} \rangle$ est un anneau commutatif.

3. Considérons un anneau quelconque $\mathcal{K} = \langle K, +, -, \cdot, 1 \rangle$. Le tableau de la forme

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

où a, b, c, d sont des éléments de K, est appelé *matrice carrée* d'ordre deux sur $\mathcal{K}$ ou matrice 2×2 sur $\mathcal{K}$. L'ensemble de toutes les matrices 2×2 sur $\mathcal{K}$ sera noté $K^{2 \times 2}$. Introduisons sur cet ensemble la relation d'égalité. Les matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ et } \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

sont dites *égales* et l'on écrit

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

si $a = e$, $b = f$, $c = g$, $d = h$.

Les matrices

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ et } \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

sont dites *matrice unité* et *matrice nulle* respectivement. Sur l'ensemble des matrices 2×2 sur $\mathcal{K}$ les opérations d'addition, de multiplication et l'opération singulaire sont définies de la façon suivante :

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} = \begin{bmatrix} a+a_1 & b+b_1 \\ c+c_1 & d+d_1 \end{bmatrix};$$

$$-\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix};$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} = \begin{bmatrix} aa_1+bc_1 & ab_1+bd_1 \\ ca_1+dc_1 & cb_1+dd_1 \end{bmatrix}.$$

On vérifie directement que l'algèbre $\langle K^{2\times 2}, +, -\rangle$ est un groupe abélien, l'algèbre $\langle K^{2\times 2}, \cdot, I\rangle$ un monoïde et le produit des matrices est distributif par rapport à l'addition. Par conséquent, l'algèbre $\langle K^{2\times 2}, +, -, \cdot, I\rangle$ est un anneau qui de plus n'est pas commutatif. Cet anneau est appelé *anneau des matrices* 2×2 *sur* $\mathcal{K}$ et l'on le désigne par le symbole $\mathcal{K}^{2\times 2}$.

Propriétés élémentaires de l'anneau. Soit $\mathcal{K}$ un anneau. Vu que l'algèbre $\langle K, +, -\rangle$ est un groupe abélien, en vertu de la propriété 3.5 pour tous éléments a, b de K l'équation $b + x = a$ possède une solution unique $a + (-b)$ notée également $a - b$.

THÉORÈME 4.1. *Soit* $\mathcal{K} = \langle K, +, -, \cdot, 1\rangle$ *un anneau. Alors pour tous éléments* a, b, c *de l'anneau* :

(1) *si* $a + b = a$, *on a* $b = 0$;

(2) *si* $a + b = 0$, *on a* $b = -a$;

(3) $-(-a) = a$;

(4) $0 \cdot a = a \cdot 0 = 0$;

(5) $(-a)\, b = a\,(-b) = -(ab)$;

(6) $(-a)(-b) = a \cdot b$;

(7) $(a - b)\, c = ac - bc$ *et* $c\,(a - b) = ca - cb$.

Démonstration. (1) Si $a + b = a$, on a

$$b = 0 + b = (-a + a) + b = -a + (a + b) = -a + a = 0.$$

(2) Si $a + b = 0$, il vient

$$b = 0 + b = (-a + a) + b = -a + (a + b) = -a + 0 = -a.$$

(3) Dans le groupe additif d'un anneau $(-a) + (-(-a)) = -a + a$. D'où, en vertu de la règle de simplification, s'ensuit l'égalité $-(-a) = a$.

7—01762

(4) En vertu de la distributivité de la multiplication par rapport à l'addition $0 \cdot a + 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a$, c'est-à-dire $0 \cdot a + 0 \cdot a = 0 \cdot a$. En vertu de (1) de la dernière égalité on déduit $0 \cdot a = 0$.

(5) En vertu de (4) et de la distributivité de la multiplication par rapport à l'addition $ab + (-a)\, b = (a + (-a))\, b = 0 \cdot b = 0$, c'est-à-dire $ab + (-a)\, b = 0$. D'où, en vertu de (2), il s'ensuit que $(-a)\, b = -(ab)$. De façon analogue on démontre que $a\,(-b) = -(ab)$.

(6) En vertu de (5) et (3) $(-a) \cdot (-b) = -((-a) \cdot b) = -(-(ab)) = a \cdot b$.

(7) En vertu de (5) et de la distributivité de la multiplication par rapport à l'addition $(a - b) \cdot c = (a + (-b)) \cdot c = a \cdot c + (-b) \times c = a \cdot c + (-b \cdot c) = a \cdot c - b \cdot c$. De façon analogue on démontre que $c \cdot (a - b) = c \cdot a - c \cdot b$. □

Homomorphismes des anneaux. En accord avec la définition de l'homomorphisme des algèbres et en rapport avec le fait que les anneaux sont un cas particulier des algèbres énonçons les définitions suivantes.

Soient $\mathscr{K} = \langle K, +, -, \circ, 1 \rangle$ et $\mathscr{K}' = \langle K', +, -, \cdot, 1' \rangle$ des anneaux. On dit que l'application h de l'ensemble K dans K' respecte les opérations principales de l'anneau $\mathscr{K}$ si sont remplies les conditions:

(1) $h\,(a + b) = h\,(a) + h\,(b)$ pour tous a, b de K;

(2) $h\,(-a) = -h\,(a)$ pour tout a de K;

(3) $h\,(a \cdot b) = h\,(a) \circ h\,(b)$ pour tous a, b de K;

(4) $h\,(1) = 1'$.

DÉFINITION. On appelle *homomorphisme de l'anneau* $\mathscr{K}$ *dans* (*sur*) *l'anneau* $\mathscr{K}'$ l'application de l'ensemble K dans (sur) K' qui respecte toutes les opérations principales de l'anneau $\mathscr{K}$. Un homomorphisme de l'anneau $\mathscr{K}$ sur $\mathscr{K}'$ est nommé *épimorphisme*.

DÉFINITION. On appelle *isomorphisme* l'homomorphisme h de l'anneau $\mathscr{K}$ sur l'anneau $\mathscr{K}'$ si h est une application injective de l'ensemble K sur K'. Les anneaux $\mathscr{K}$ et $\mathscr{K}'$ sont dits *isomorphes* s'il existe un isomorphisme de l'anneau $\mathscr{K}$ sur $\mathscr{K}'$.

La notation $\mathscr{K} \cong \mathscr{K}'$ signifie que les anneaux $\mathscr{K}$ et $\mathscr{K}'$ sont isomorphes.

DÉFINITION. On appelle *monomorphisme* ou *injection* l'homomorhisme h de l'anneau $\mathscr{K}$ dans l'anneau $\mathscr{K}'$ si h est une application injective de l'ensemble K dans K'.

DÉFINITION. On appelle *endomorphisme de l'anneau* $\mathscr{K}$ l'homomorphisme de l'anneau $\mathscr{K}$ en lui-même. Un isomorphisme de l'anneau $\mathscr{K}$ en lui-même est nommé *automorphisme de l'anneau* $\mathscr{K}$.

Ainsi, par exemple, on considère comme automorphisme l'application identique de l'anneau sur lui-même.

Théorème 4.2. *Si une application h de l'anneau* $\mathcal{K}$ *dans l'anneau* $\mathcal{K}'$ *fait passer l'unité de l'anneau* $\mathcal{K}$ *en l'unité de l'anneau* $\mathcal{K}'$ *tout en respectant les opérations d'addition et de multiplication, c'est-à-dire que*

$$h(x+y) = h(x) + h(y) \text{ pour tous } x, y \text{ de } K,$$

$$h(xy) = h(x) \circ h(y) \text{ pour tous } x, y \text{ de } K,$$

alors h fait passer le zéro de l'anneau $\mathcal{K}$ *en zéro de l'anneau* $\mathcal{K}'$ *et est un homomorphisme.*

Démonstration. Considérons des groupes additifs

$$\langle K, +, - \rangle \text{ et } \langle K', +, - \rangle$$

d'anneaux $\mathcal{K}$ et $\mathcal{K}'$. Par hypothèse, h respecte l'opération d'addition. D'où, en vertu du théorème 3.1, il s'ensuit que h fait passer le zéro de l'anneau $\mathcal{K}$ en zéro de l'anneau $\mathcal{K}'$ et est un homomorphisme du groupe $\langle K, +, - \rangle$ dans le groupe $\langle K', +, - \rangle$. En particulier, $h(-x) = -h(x)$ pour tout x de K. Par conséquent, l'application h respecte toutes les opérations principales de l'anneau $\mathcal{K}$ et est un homomorphisme. □

Théorème 4.3. *Une relation d'isomorphisme sur un ensemble quelconque d'anneaux est réflexive, transitive et symétrique et, par suite, est une relation d'équivalence.*

Ce théorème découle directement du théorème 2.5.

Exemples. 1. Considérons un ensemble Q des nombres rationnels, $Q[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Q\}$. L'algèbre $\mathcal{Q}[\sqrt{2}] = \langle Q[\sqrt{2}], +, -, \cdot, 1 \rangle$ est un anneau. L'application $f\colon Q[\sqrt{2}] \to Q[\sqrt{2}]$ définie par la formule $f(a + b\sqrt{2}) = a - b\sqrt{2}$ est une application injective de l'ensemble $Q[\sqrt{2}]$ sur lui-même. L'application f respecte les opérations principales de l'anneau $Q[\sqrt{2}]$. En effet, pour tous $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$

$$f(xy) = f\big(ac + 2bd + (ad + bc)\sqrt{2}\big) = (ac + 2bd) - (ad + bc)\sqrt{2} =$$
$$= (a - b\sqrt{2})(c - d\sqrt{2}) = f(x) f(y);$$

$$f(x+y) = f\big(a + b\sqrt{2} + c + d\sqrt{2}\big) = a - b\sqrt{2} + b - d\sqrt{2} =$$
$$= f(x) + f(y);$$

$$f(1_{\mathcal{Q}}) = 1 = 1_{\mathcal{Q}[\sqrt{2}]}.$$

Par conséquent, l'application f est un automorphisme de l'anneau $\mathcal{Q}[\sqrt{2}]$.

2. Soient K un ensemble de toutes les matrices de la forme $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$ à a et b rationnels et $\mathscr{K} = \langle K, +, -, \cdot, 1 \rangle$, anneau de telles matrices. L'application h: $Q[\sqrt{2}] \to K$ définie par la formule

$$h(a + b\sqrt{2}) = \begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$$

constitue une application injective de l'ensemble $Q[\sqrt{2}]$ sur K. On vérifie sans peine que l'application h respecte les opérations principales de l'anneau $\mathscr{Q}[\sqrt{2}]$. h est donc un isomorphisme de l'anneau $\mathscr{Q}[\sqrt{2}]$ sur l'anneau $\mathscr{K}$.

3. Soit L l'ensemble de toutes les matrices de la forme $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ nommées *diagonales* avec a et b rationnels. L'algèbre $\mathscr{L} = \langle L, +, -, \cdot, I \rangle$, où $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ est un anneau. L'application f: $L \to Q$ définie par la formule

$$f\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\right) = a \text{ pour tous } a, b \text{ de } Q$$

est une application respectant les opérations principales de l'anneau $\mathscr{L}$. Par conséquent, f est un homomorphisme de l'anneau $\mathscr{L}$ sur l'anneau $\mathscr{Q}$ des nombres rationnels.

Sous-anneaux. Soit $\mathscr{K} = \langle K, +, -, \cdot, 1 \rangle$ un anneau.

DÉFINITION. On appelle *sous-anneau de l'anneau* $\mathscr{K}$ toute sous-algèbre de cet anneau.

En accord avec la définition de la sous-algèbre on est en mesure de définir un sous-anneau en plus de détails de la façon suivante.

L'algèbre $\mathscr{L} = \langle L, \oplus, \ominus, \odot, 1_{\mathscr{L}} \rangle$ du type (2, 1, 2, 0) se nomme *sous-anneau de l'anneau* $\mathscr{K}$ si $L \subset K$ et si l'application identique de l'ensemble L dans K est un monomorphisme de l'algèbre $\mathscr{L}$ dans $\mathscr{K}$, c'est-à-dire si sont remplies les conditions:

(1) $a \oplus b = a + b$ pour tous a, b de L;

(2) $\ominus a = -a$ pour tout a de L;

(3) $a \odot b = a \cdot b$ pour tous a, b de L;

(4) $1_{\mathscr{L}} = 1_{\mathscr{K}}$.

La notation $\mathscr{L} \dashv\!\!\!\!3\ \mathscr{K}$ signifie que l'algèbre $\mathscr{L}$ est un sous-anneau de l'anneau $\mathscr{K}$.

Si $\mathscr{L} \dashv\!\!\!\!3\ \mathscr{K}$ il s'ensuit de la définition du sous-anneau que l'ensemble L est clos par rapport à chaque opération principale de l'an-

neau $\mathcal{K}$, autrement dit, l'application de toute opération principale de l'anneau $\mathcal{K}$ aux éléments de L aboutit de nouveau aux éléments de l'ensemble L. En outre, en vertu des conditions (1)-(4) chaque opération principale de l'algèbre $\mathcal{L}$ est une restriction de l'opération principale appropriée de l'anneau $\mathcal{K}$ par l'ensemble L.

THÉORÈME 4.4. *Tout sous-anneau d'un anneau est un anneau. Le zéro et l'unité de l'anneau constituent le zéro et l'unité de tout son sous-anneau.*

D é m o n s t r a t i o n. Soient $\mathcal{L} = \langle L, \oplus, \ominus, \odot, 1_{\mathcal{L}} \rangle$ un sous-anneau de l'anneau $\mathcal{K} = \langle K, +, -, \cdot, 1 \rangle$ et 0 le zéro de l'anneau $\mathcal{K}$. En vertu des conditions (1) et (2) l'algèbre $\langle L, \oplus, \ominus \rangle$ est un sous-groupe du groupe additif $\langle K, +, - \rangle$ de l'anneau $\mathcal{K}$. Donc l'algèbre $\langle L, \oplus, \ominus \rangle$ est un groupe abélien et 0 son élément zéro.

Dans $\mathcal{L}$ la multiplication est associative. En effet, en vertu de (3), il vient

$$a \odot (b \odot c) = a \cdot (b \cdot c) = (a \cdot b) \cdot c = (a \odot b) \odot c$$

pour tous a, b, c de L. En vertu de (3) et (4) $1_{\mathcal{L}} = 1$ et $a \odot 1_{\mathcal{L}} = a \odot 1 = a \cdot 1 = a$ pour tout a de L. Par conséquent, l'algèbre $\langle L, \odot, 1_{\mathcal{L}} \rangle$ est un monoïde.

Dans $\mathcal{L}$ la multiplication est distributive par rapport à l'addition. En effet, en vertu de (1) et (3), pour tous a, b, c de L

$$(a \oplus b) \odot c = (a + b) \cdot c = a \cdot c + b \cdot c = a \odot b \oplus b \odot c$$

et, de façon analogue, on a $c \odot (a \oplus b) = \cdot c \odot a \oplus c \odot b$. Donc, l'algèbre $\mathcal{L}$ est un anneau. □

Considérons un anneau $\mathcal{K} = \langle K, +, -, \cdot, 1 \rangle$ et A un sous-ensemble quelconque non vide de l'ensemble K fermé aux opérations principales de l'anneau $\mathcal{K}$. Soient $\oplus$, $\ominus$, $\odot$ une restriction des opérations principales de l'anneau $\mathcal{K}$ à l'ensemble A, c'est-à-dire

$a \oplus b = a + b$ pour tous a, b de A;

$\ominus a = -a$ pour tout a de A;

$a \odot b = ab$ pour tous a, b de A.

Alors, suivant les théorèmes 2.6 et 4.4 l'algèbre $\mathcal{A}$

(5) $\mathcal{A} = \langle A, \oplus, \ominus, \odot, 1 \rangle$,

est un sous-anneau de l'anneau $\mathcal{K}$. Ainsi le sous-anneau $\mathcal{A}$ de l'anneau $\mathcal{K}$ se définit de façon univoque par un sous-ensemble non vide A de l'ensemble K clos dans $\mathcal{K}$. Aussi au lieu de (5) écrit-on: « le sous-anneau $\mathcal{A} = \langle A, +, -, \cdot, 1 \rangle$ » et lit-on « l'ensemble A est un sous-anneau de l'anneau $\mathcal{K}$ par rapport aux opérations $+$, $-$, $\cdot$, 1 ».

THÉORÈME 4.5. *La relation binaire* $\dashv$ (« *constituer un sous-anneau* ») *sur un ensemble de sous-anneaux de l'anneau donné est réflexive, transitive et antisymétrique, c'est-à-dire est une relation d'ordre non strict.*

Ce théorème est un cas particulier du théorème 2.8.

THÉORÈME 4.6. *L'intersection d'une collection quelconque (non vide) de sous-anneaux de l'anneau* $\mathcal{K}$ *est un sous-anneau de l'anneau* $\mathcal{K}$.

Ce théorème est un cas particulier du théorème 2.10.

Il s'ensuit du théorème 4.4 que pour tout ensemble M d'éléments de l'anneau $\mathcal{K}$ il y a un sous-anneau $\mathcal{L}$ minimal incluant l'ensemble M. On voit sans peine que $\mathcal{L}$ est l'intersection de tous les sous-anneaux de l'anneau $\mathcal{K}$ comprenant l'ensemble M. Ce sous-anneau minimal $\mathcal{L}$ est nommé *sous-anneau engendré par l'ensemble* M, M étant le *système de génératrices* pour l'anneau $\mathcal{L}$.

E x e m p l e s. 1. Soit D l'ensemble de toutes les matrices 2×2 diagonales de la forme $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ associées à l'anneau $\mathcal{K}$. L'ensemble D est férme aux opérations principales de l'anneau de toutes les matrices 2×2 associées à l'anneau K, $\mathcal{K}^{2\times 2} = \langle K^{2\times 2}, +, -, \cdot, I\rangle$. L'algèbre $\langle D, +, -, \cdot, 1\rangle$ est donc un sous-anneau de l'anneau $\mathcal{K}^{2\times 2}$.

2. Les matrices de la forme $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ sont nommées *matrices triangulaires supérieures*. Soit L l'ensemble de toutes les matrices triangulaires supérieures associées à l'anneau $\mathcal{K} = \langle K, +, -, \cdot, 1\rangle$. L'ensemble L est fermé aux opérations principales de l'anneau $\mathcal{K}^{2\times 2} = \langle K^{2\times 2}, +, -, \cdot, I\rangle$ des matrices 2×2 sur $\mathcal{K}$. Par conséquent, l'algèbre $\langle L, +, -, \cdot, I\rangle$ est un sous-anneau de l'anneau $\mathcal{K}^{2\times 2}$.

3. Soient $\mathcal{K}$ un anneau quelconque non nul et S l'ensemble de toutes les matrices de la forme $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ aux éléments a, b de K. En vérifiant directement on voit que l'ensemble S est fermé aux opérations principales de l'anneau $\mathcal{K}^{2\times 2} = \langle K^{2\times 2}, +, -, \cdot, I\rangle$. L'algèbre $\langle S, +, -, \cdot, I\rangle$ est donc un sous-anneau de l'anneau $\mathcal{K}^{2\times 2}$.

4. Soit $\mathcal{K} = \langle K, +, -, \cdot, 1\rangle$ un anneau de toutes les fonctions réelles définies et continues sur l'ensemble **R** des nombres réels. Soit D l'ensemble de toutes les fonctions réelles définies et dérivables sur l'ensemble **R**. L'ensemble D est fermé aux opérations principales de l'anneau $\mathcal{K}$. Donc, l'algèbre $\langle D, +, -, \cdot, 1\rangle$ est un sous-anneau de l'anneau $\mathcal{K}$.

Exercices

1. Elucider si les ensembles suivants des nombres rationnels sont clos relativement aux opérations principales de l'anneau des nombres rationnels:
(a) l'ensemble de tous les entiers pairs;
(b) l'ensemble de tous les nombres naturels;
(c) l'ensemble de tous les nombres rationnels dont les dénominateurs sont l'unité ou des nombres pairs;
(d) l'ensemble de tous les nombres rationnels aux dénominateurs impairs.

2. Elucider si les ensembles suivants des nombres réels sont clos relativement aux opérations principales de l'anneau de tous les nombres réels:
(a) l'ensemble de tous les nombres de la forme $a + b\sqrt{2}$ à a et b entiers;
(b) l'ensemble de tous les nombres de la forme $a + b\sqrt{3}$ à a et b entiers;
(c) l'ensemble de tous les nombres de la forme $a + b\sqrt{5}$ à a et b rationnels.

3. Considérer un anneau non nul $\mathcal{K}$. Démontrer que l'anneau des matrices 2×2 sur $\mathcal{K}$ est un anneau non commutatif avec diviseurs de zéro.

4. Démontrer que dans l'anneau composé de n éléments pour chaque élément a de l'anneau $na = 0$.

5. Démontrer que si l'élément a de l'anneau est permutable avec l'élément b, c'est-à-dire que $ab = ba$, il est également permutable avec les éléments $(-b)$, b^{-1} et nb, où n est un entier; si l'élément a est permutable avec les éléments b et c il est également permutable avec les éléments $b + c$ et bc.

6. Soit $a^2 = a$ pour chaque élément a de l'anneau $\mathcal{K}$. Montrer que l'anneau $\mathcal{K}$ est commutatif.

7. Soit f un homomorphisme de l'anneau $\mathcal{K}$ dans l'anneau $\mathcal{K}' = \langle K', +, -, \cdot, 1\rangle$. Montrer que l'algèbre $\langle \mathrm{Im}\, f, +, -, \cdot, 1\rangle$ est un sous-anneau de l'anneau $\mathcal{K}'$.

8. Démontrer que pour tous éléments x, y d'un anneau commutatif et des entiers positifs quelconques m et n
(a) $x^m \cdot x^n = x^{m+n}$; (b) $(x^m)^n = x^{mn}$; (c) $(xy)^n = x^n y^n$.

9. Démontrer que l'algèbre isomorphe à l'anneau est elle-même un anneau.

10. Démontrer pour un anneau quelconque en recourant à la récurrence par n le théorème binomial

$$(a+b)^n = a^n + C_n^1 a^{n-1}b + C_n^2 a^{n-2}b^2 + \ldots + b^n,$$

où n est un entier positif et $C_n^k = \dfrac{n!}{k!\,(n-k)!}$.

§ 5. Systèmes algébriques

Notion de système algébrique. Soit A un ensemble non vide quelconque.

DÉFINITION. On appelle *système algébrique* un triplet ordonné

$$\mathcal{A} = \langle A, \Omega, \Omega_0\rangle,$$

où A est un ensemble non vide, Ω l'ensemble d'opérations sur A et Ω_0 l'ensemble de relations sur A.

Un système algébrique $\mathcal{A}$ est donc défini par trois ensembles:

(a) un ensemble non vide A noté également $|\mathcal{A}|$; cet ensemble est nommé *ensemble de base du système* $\mathcal{A}$ et ses éléments *éléments du système* $\mathcal{A}$;

(b) un ensemble d'opérations Ω définies sur A et appelées *opérations principales du système* $\mathcal{A}$;

(c) un ensemble de relations Ω_0 données sur A et nommées *relations principales du système* $\mathcal{A}$.

Si $\langle A, \Omega, \Omega_0\rangle$ est un système algébrique on dit aussi que l'ensemble A est un système algébrique par rapport aux opérations Ω et aux relations Ω_0.

On comprend parfois par système algébrique le couple $\langle A, \Omega^*\rangle$, où $\Omega^* = \Omega \cup \Omega_0$, Ω étant l'ensemble des opérations sur A, et Ω_0 l'ensemble des relations sur A. Dans ce cas si $\Omega_0 = \varnothing$, le système $\langle A, \Omega^*\rangle = \langle A, \Omega\rangle$ est alors une algèbre. On peut donc ainsi considérer l'algèbre comme un cas particulier du système algébrique.

DÉFINITION. Les systèmes algébriques $\mathcal{A} = \langle A, \Omega, \Omega_0\rangle$ et $\mathcal{B} = \langle B, \Omega', \Omega_0'\rangle$ sont dits *du même type* si les algèbres $\langle A, \Omega\rangle$ et $\langle B, \Omega'\rangle$ sont du même type et qu'il existe une application injective de l'ensemble Ω_0 sur Ω_0' pour laquelle toute relation $R_{\mathcal{A}}$ de Ω_0 ainsi que la relation $R_{\mathcal{B}}$ de Ω_0' qui lui correspond dans l'application sont du même rang.

Le cas rencontré le plus souvent est celui d'ensembles Ω et Ω_0 finis: $\Omega = \{f_1, \ldots, f_s\}$, $\Omega_0 = \{R_1, \ldots, R_t\}$. Au lieu de la notation

$$\mathcal{A} = \langle A, \{f_1, \ldots, f_s\}, \{R_1, \ldots, R_t\}\rangle$$

on utilise habituellement la notation

$$\mathcal{A} = \langle A, f_1, \ldots, f_s, R_1, \ldots, R_t\rangle.$$

En outre la suite $(\mathrm{r}\,(f_1), \ldots, \mathrm{r}\,(f_s); \mathrm{r}\,(R_1), \ldots, \mathrm{r}\,(R_t))$, où $\mathrm{r}\,(f_i)$ est le rang de l'opération f_i et $\mathrm{r}\,(R_k)$ le rang de la relation R_k, est nommée *type du système* $\mathcal{A}$. Les systèmes algébriques $\mathcal{A}$ et $\mathcal{B}$,

$$\mathcal{B} = \langle B, f_1', \ldots, f_s', R_1', \ldots, R_t'\rangle,$$

sont du *même type* si leurs types coïncident, c'est-à-dire si $\mathrm{r}\,(f_i) = \mathrm{r}\,(f_i')$ pour $i = 1, \ldots, s$, $\mathrm{r}\,(R_1) = \mathrm{r}\,(R_k')$ pour $k = 1, \ldots, t$. En outre, l'opération f_i' du système $\mathcal{B}$ est dite *opération associée à l'opération* f_i du système $\mathcal{A}$, tandis que la relation R_k' du système $\mathcal{B}$ est nommée *relation associée à la relation* R_k du système $\mathcal{A}$.

E x e m p l e. Un ensemble de nombres naturels N avec des opérations banales d'addition $+$, de multiplication $\cdot$ et la relation d'ordre $\leqslant$ est un système algébrique $\langle \mathrm{N}, +, \cdot, \leqslant\rangle$ du type (2, 2; 2).

Isomorphismes des systèmes algébriques. Soient $\mathcal{A}$ et $\mathcal{B}$ des systèmes algébriques du même type, $R_{\mathcal{A}}$ une relation principale arbitraire du système $\mathcal{A}$ et $R_{\mathcal{B}}$ la relation principale appropriée du système $\mathcal{B}$. On dit que l'application h de l'ensemble $|\mathcal{A}|$ dans $|\mathcal{B}|$

respecte la relation $R_{\mathscr{A}}$ si

$$(a_1, \ldots, a_n) \in R_{\mathscr{A}} \leftrightarrow (h(a_1), \ldots, h(a_n)) \in R_{\mathscr{B}}$$

pour tous $a_1, \ldots, a_n$ de $|\mathscr{A}|$,

où n est le rang de la relation $R_{\mathscr{A}}$.

DÉFINITION. On appelle *isomorphisme du système algébrique* $\mathscr{A}$ sur un système du même type $\mathscr{B}$ l'application injective de l'ensemble $|\mathscr{A}|$ sur $|\mathscr{B}|$ respectant toutes les opérations et relations principales du système $\mathscr{A}$. Les systèmes $\mathscr{A}$ et $\mathscr{B}$ sont dits *isomorphes* s'il y a isomorphisme du système $\mathscr{A}$ sur $\mathscr{B}$.

La notation $\mathscr{A} \cong \mathscr{B}$ signifie que les systèmes $\mathscr{A}$ et $\mathscr{B}$ sont isomorphes.

DÉFINITION. On appelle *monomorphisme* ou *injection* du système algébrique $\mathscr{A}$ dans un système $\mathscr{B}$ du même type l'application injective de l'ensemble $|\mathscr{A}|$ dans $|\mathscr{B}|$ qui respecte toutes les opérations et relations principales du système $\mathscr{A}$.

DÉFINITION. On appelle *homomorphisme du système algébrique* $\mathscr{A}$ *dans le système* $\mathscr{B}$ *du même type* l'application h de l'ensemble $|\mathscr{A}|$ dans $|\mathscr{B}|$ qui respecte toutes les opérations principales du système $\mathscr{A}$ et qui satisfait à la condition

$$(a_1, \ldots, a_n) \in R_{\mathscr{A}} \rightarrow (h(a_1), \ldots, h(a_n)) \in R_{\mathscr{B}}$$

pour tous $a_1, \ldots, a_n$ de $|\mathscr{A}|$,

où $R_{\mathscr{A}}$ est une relation principale quelconque du système $\mathscr{A}$, n son rang, tandis que $R_{\mathscr{B}}$ est la relation principale du système $\mathscr{B}$ associée à la relation $R_{\mathscr{A}}$.

Sous-systèmes. Soient $\mathscr{A}$ et $\mathscr{B}$ des systèmes algébriques du même type, $f_{\mathscr{A}}$ l'opération principale du système $\mathscr{A}$ et $f_{\mathscr{B}}$ l'opération principale appropriée du système $\mathscr{B}$, $R_{\mathscr{A}}$ la relation principale du système $\mathscr{A}$ et $R_{\mathscr{B}}$ la relation principale appropriée du système $\mathscr{B}$.

DÉFINITION. Le système $\mathscr{A}$ est nommé *sous-système du système* $\mathscr{B}$ si $|\mathscr{A}| \subset |\mathscr{B}|$ et pour chaque opération principale $f_{\mathscr{A}}$ et chaque relation principale $R_{\mathscr{A}}$ sont remplies les conditions:

$$(1) \quad f_{\mathscr{A}}(a_1, \ldots, a_m) = f_{\mathscr{B}}(a_1, \ldots, a_m)$$

pour tous $a_1, \ldots, a_m$ de $|\mathscr{A}|$,

$$(2) \quad (a_1, \ldots, a_n) \in R_{\mathscr{A}} \leftrightarrow (a_1, \ldots, a_n) \in R_{\mathscr{B}}$$

pour tous $a_1, \ldots, a_n$ de $|\mathscr{A}|$,

où m est le rang de l'opération $f_{\mathscr{A}}$ et n le rang de la relation $R_{\mathscr{A}}$.

Autrement dit, le système $\mathcal{A}$ est appelé *sous-système du système* $\mathcal{B}$ si $|\mathcal{A}| \subset |\mathcal{B}|$ et l'application identique de $|\mathcal{A}|$ dans $|\mathcal{B}|$ est un monomorphisme du système $\mathcal{A}$ dans le système $\mathcal{B}$. La notation $\mathcal{A} \dashv \mathcal{B}$ signifie que le système $\mathcal{A}$ est un sous-système du système $\mathcal{B}$.

Il s'ensuit de la définition que si $\mathcal{A} \dashv \mathcal{B}$, l'ensemble $|\mathcal{A}|$ est clos dans le système $\mathcal{B}$ et, par suite, que l'application de toute opération principale $f_{\mathcal{B}}$ aux éléments de l'ensemble $|\mathcal{A}|$ aboutit de nouveau aux éléments de l'ensemble $|\mathcal{A}|$. En vertu de (1), chaque opération principale $f_{\mathcal{A}}$ de l'algèbre $\mathcal{A}$ est une restriction de l'opération appropriée $f_{\mathcal{B}}$ par l'ensemble $|\mathcal{A}|$, c'est-à-dire qu'on a $f_{\mathcal{A}} = f_{\mathcal{B}} \| \mathcal{A} |$.

Soient R une relation de rang n sur l'ensemble B et $A \subset B$.

Définition. La relation S de rang n sur l'ensemble A est appelée *restriction de la relation R par l'ensemble A* si $S = R \cap A^n$, ce qui est équivalent à la condition

$$(a_1, \ldots, a_n) \in S \leftrightarrow (a_1, \ldots, a_n) \in R$$

pour tous $a_1, \ldots, a_n$ de A.

Il s'ensuit de cette définition en vertu de (2), que chaque relation principale d'une sous-algèbre est une restriction de sa relation appropriée par l'algèbre même.

Soient $\mathcal{B} = \langle B, f_1, \ldots, f_s, R_1, \ldots, R_t \rangle$ un système algébrique et C un sous-ensemble quelconque non vide de l'ensemble $|\mathcal{B}|$ clos relativement aux opérations principales du système $\mathcal{B}$. Notons $f_i \mid C$ et $R_k \mid C$ les restrictions par l'ensemble C de l'opération f_i et de la relation R_k respectivement ($i = 1, \ldots, s$; $k = 1, \ldots, t$). Le système

$$(3) \quad \mathcal{C} = \langle C, f_1 \mid C, \ldots, f_s \mid C, R_1 \mid C, \ldots, R_t \mid C \rangle$$

est un sous-système du système $\mathcal{B}$. Donc, le sous-système $\mathcal{C}$ du système $\mathcal{B}$ est défini de façon univoque par le sous-ensemble non vide C clos dans le système $\mathcal{B}$. Aussi au lieu de (3) écrit-on: « le sous-système $\mathcal{C} = \langle C, f_1, \ldots, f_s; R_1, \ldots, R_t \rangle$ » ou bien « l'ensemble C est un sous-système relativement aux opérations $f_1, \ldots, f_s$ et aux relations $R_1, \ldots, R_t$ ».

Exercices

1. Soit h un isomorphisme d'un système algébrique $\langle A, R \rangle$ sur le système algébrique $\langle B, S \rangle$, où R et S sont des relations binaires. Démontrer qu'on a alors:

(a) si R est réflexif (sur A), S est aussi réflexif (sur B);
(b) si R n'est pas réflexif (sur A), S n'est également pas réflexif (sur B);
(c) si la relation R est symétrique, S l'est également;
(d) si R est transitif, S l'est également;

(e) si R est antisymétrique, S l'est également;

(f) si R est lié, S l'est également;

(g) si R est une relation d'ordre strict (non strict) (sur A), S est aussi une relation d'ordre strict (non strict) (sur B);

(h) si R est une relation d'ordre total (sur A), S est aussi une relation d'ordre total (sur B).

2. Montrer sur l'exemple des systèmes $\langle \mathbf{N}, \sigma \rangle$ et $\langle \mathbf{N}, > \rangle$, où σ est une relation binaire vide sur $\mathbf{N}$, quant à $\mathbf{N}$, c'est l'ensemble des nombres naturels, que chaque homomorphisme mutuellement univoque n'est pas un isomorphisme.

3. Donner des exemples d'isomorphismes et d'homomorphismes de systèmes algébriques.

CHAPITRE IV

PRINCIPAUX SYSTÈMES NUMÉRIQUES

§ 1. Système des nombres naturels

Alphabet et mots. On appelle *alphabet* une collection arbitraire de symboles nommés *lettres.* On admet aussi que les lettres peuvent être répétées un nombre infini de fois comme des caractères d'imprimerie. La série des lettres de l'alphabet peut être énoncée sous forme d'une liste concrète de lettres enserrées entre des accolades. Il est admis que dans une telle liste il ne peut y avoir de répétitions : toutes deux lettres de l'alphabet sont différentes. Posons que chaque alphabet possède au moins une lettre.

Les lettres composant l'alphabet $\mathfrak{A}$ sont nommées *lettres de l'alphabet* $\mathfrak{A}$. On dit aussi des lettres de l'alphabet $\mathfrak{A}$ qu'elles appartiennent à $\mathfrak{A}$.

Toute suite finie de lettres est appelée *mot.* Dans l'alphabet $\mathfrak{A}$ donné on dénomme mot chaque lettre appartenant à cet alphabet. Par exemple, les mots *a*, *ba*, *baab*, *baaacb* sont des mots de l'alphabet $\{a, b, c\}$. Les mots 0, 00, 0 |, |, 0 | 0 |, || 00 peuvent être considérés comme des mots de l'alphabet {0, |}. Vu que chaque suite de lettres d'un alphabet écrites l'une à la suite de l'autre est un mot, dans tout alphabet considéré il peut y avoir des mots de longueur aussi grande que l'on veut. Il est commode d'introduire dans l'étude un mot ne contenant aucune lettre ; un tel mot est nommé *mot vide.*

Deux mots sont dits *égaux* (égaux graphiquement) si leur écriture coïncide, c'est-à-dire s'ils sont composés des mêmes lettres se disposant identiquement.

Supposons que les symboles A et B désignent des mots dans un alphabet quelconque. Associons au couple A, B le mot AB qu'on obtient en écrivant à la suite du mot A (à droite) le mot B. Le mot AB est dit *composition* (concaténation) ou *assemblage* des mots A et B. Par exemple, si A désigne le mot *bac*, et B le mot *aba*, AB désignera le mot *bacaba.* La composition de tout mot A avec un mot vide, par définition, est considérée égale au mot A.

On se convainc sans peine que la concaténation (composition) de mots est associative : pour trois mots quelconques A, B, C la composition des mots AB et C est égale à la composition des mots A et BC.

Aussi les deux compositions peuvent-elles être notées de la même façon: ABC.

Le mot B est dit *inversion* (*par miroir*) *du mot A* si B est composé des mêmes occurrences de lettres que A, mais écrites dans un ordre inverse. Par exemple, le mot *bac* est une inversion du mot *cab*, et réciproquement. Un mot est dit *symétrique* s'il coïncide avec son inversion, par exemple, les mots *sis*, *bab*, $0 \mid 0$ sont des mots symétriques.

Le mot A est dit *sous-mot du mot B* s'il existe des mots C et E (probablement vides) tels que $B = CAE$. Si A est un sous-mot de B, on dit que A apparaît dans B. Pour des mots A et B donnés le mot A peut posséder plusieurs occurrences dans le mot B. Il est clair qu'un mot vide est sous-mot de tout mot.

Mots d'un alphabet à lettre unique. Considérons un alphabet $r = \{ \mid \}$ composé d'une seule lettre « | » nommée bâton vertical. Notons N^* l'ensemble de tous les mots de l'alphabet r à une lettre. A l'ensemble N^* appartiennent le mot vide noté 0^*, les mots |, ||, |||, ||||, etc. Si n est un mot de l'alphabet r, $n \mid$ est également un mot de cet alphabet.

Deux éléments m et n de N^* sont dits *égaux* et l'on écrit $m = n$ s'ils sont égaux comme des mots (égaux graphiquement). Si les mots m et n ne sont pas égaux, on écrit $m \neq n$.

DÉFINITION. Soient m et n des mots quelconques de l'alphabet r. La composition des mots m et n porte le nom de *somme* de m et n et est notée $m \oplus n$. L'opération $\oplus$ est nommée *opération d'addition*.

Par exemple, la composition des mots || et ||| est le mot |||||. Donc, $|| \oplus ||| = |||||$.

La composition d'un mot quelconque n de N^* et d'un mot vide 0^* est par définition le mot n. Donc, $n \oplus 0^* = n$, $0^* + n = n$.

On a mentionné plus haut qu'une composition de mots est associative. En particulier, pour tous éléments m et n de N^* se vérifie l'égalité $m \oplus (n \oplus |) = (m \oplus n) \oplus |$ ou, puisque $n \oplus | = n \mid$, $m \oplus n \mid = (m \oplus n) \mid$. L'associativité de la composition des mots permet de déterminer la somme de trois termes et plus:

$$k \oplus m \oplus n = (k \oplus m) \oplus n, \quad k \oplus m \oplus n \oplus l = (k \oplus m \oplus n) \oplus l, \text{ etc.}$$

DÉFINITION. On appelle *produit de deux mots m et n* ($n \neq 0$) le mot égal à la somme de n termes, dont chacun est égal à m. De plus, on pose que $m \odot 0^* = 0^*$.

Le produit des mots m et n se note par $m \odot n$. L'opération $\odot$ est nommée *multiplication des mots*. On a ainsi

$$m \odot n = \underbrace{m \oplus m \oplus \ldots \oplus m}_{n \text{ fois}}.$$

Par exemple, pour tout m de N^*, il vient:

$$m \odot | = m, \quad m \odot || = m \oplus m,$$

$$m \odot ||| = m \oplus m \oplus m, \text{ etc.}$$

Système des nombres naturels. Voyons l'approche axiomatique de l'introduction des nombres naturels.

Définition. On appelle *système des nombres naturels* l'algèbre $\langle \mathbf{N}, +, \cdot, 0, 1 \rangle$ composée d'un certain ensemble **N**, d'éléments 0 et 1 séparés de **N**, d'opérations binaires $+$ et $\cdot$ (nommées addition et multiplication) satisfaisant aux conditions suivantes (axiomes):

I. Pour tout n de **N** $n + 1 \neq 0$.

II. Pour tous m et n de **N** si $m + 1 = n + 1$, on a $m = n$.

III. Pour tout m de **N** $m + 0 = m$.

IV. Pour tous m et n $m + (n + 1) = (m + n) + 1$.

V. Pour tout m de **N** $m \cdot 0 = 0$.

VI. Pour tous m et n de **N** $m \cdot (n + 1) = m \cdot n + m$.

VII. Si A est un sous-ensemble de l'ensemble **N** tel que (a) $0 \in A$, (b) pour tout n, si $n \in A$, on a aussi $n + 1 \in A$, alors on a de même $A = \mathbf{N}$.

Le système d'axiomes sus-mentionné est nommé *système d'axiomes de Peano* vu que c'est une variante insensible de l'axiomatique proposée par le mathématicien italien Peano.

La condition I signifie que l'élément 0 ne peut être représenté sous forme de somme d'un élément quelconque de **N** et de l'élément 1. La condition II veut dire que l'élément 1 est régulier à gauche par rapport à l'addition. La condition III indique que 0 est l'élément neutre à droite par rapport à l'addition. La condition IV traduit la forme faible de l'associativité de l'addition. La condition VI est une forme faible de la distributivité de la multiplication par rapport à l'addition. La condition VII est nommée *axiome de l'induction mathématique*. A partir de cet axiome s'ensuit le fait que tout sous-ensemble de l'ensemble **N** contenant 0, 1 et clos par rapport à l'addition coïncide avec l'ensemble **N**. C'est ainsi que de l'axiome d'induction mathématique il découle que l'unique sous-algèbre de l'algèbre $\mathcal{N} = \langle \mathbf{N}, +, \cdot, 0, 1 \rangle$ est l'algèbre $\mathcal{N}$ elle-même.

Les éléments de l'ensemble **N** sont appelés nombres naturels. Les éléments 0 et 1 sont nommés respectivement *zéro* et *unité du système* $\mathcal{N}$.

Pour la notation des nombres $1 + 1, (1 + 1) + 1, ((1 + 1) + 1) + 1, (((1 + 1) + 1) + 1) + 1, \ldots$ on se sert de la symbolique décimale banale: 2, 3, 4, 5, . . .

Il se pose une question : existe-t-il au moins un système des nombres naturels, c'est-à-dire une algèbre du type (2, 2, 0, 0) satisfaisant aux axiomes I-VII ? L'exemple suivant fournit une réponse affirmative à la question posée.

Considérons l'ensemble N^* d'un alphabet r à une lettre. On a déjà défini les opérations $\oplus$ et $\odot$ sur les mots de l'alphabet r. Supposons que le mot vide 0^* et le mot $|$ jouent respectivement le rôle de zéro et de l'unité dans l'algèbre:

$$\mathcal{N}^* = \langle N^*, \oplus, \odot, 0^*, |\rangle.$$

Cette algèbre satisfait au système d'axiomes I-VII. En effet, pour tout n de N^* le mot $n\,|$ n'est pas vide; donc, $n \oplus | \neq 0^*$ et, partant, la condition I est satisfaite. Puisque pour tous $m, n \in N^*$ de l'égalité graphique des mots $m\,|$ et $n\,|$ s'ensuit l'égalité graphique des mots m et n, la condition II est remplie. La composition de tout mot m de N^* et du mot vide 0^* est le mot m, $m \oplus 0^* = m$, c'est-à-dire que la condition III est satisfaite. De l'associativité de la composition des mots on déduit que la condition IV est remplie. La satisfaction de la condition V s'ensuit directement de la définition de l'opération de multiplication des mots. De l'égalité graphique des mots

$$\underbrace{mm \ldots m}_{n+1 \text{ fois}} \quad \text{et} \quad \underbrace{mm \ldots mm}_{n \text{ fois}}$$

s'ensuit l'égalité $m \odot (n \oplus |) = (m \odot n) \oplus m$, donc la condition VI est également remplie. Enfin, il est intuitivement évident que pour l'algèbre $\mathcal{N}^*$ l'axiome d'induction est satisfaite: si l'ensemble $A \subset N^*$ est tel que (a) $0^* \in A$ et (b) pour chaque n, si $n \in A$, $n\,| \in A$ et, par suite, $A = N^*$. En effet, désignons par $A(n)$ le prédicat « $n \in A$ »; écrivons pour tout n la suite d'implications vraies en vertu de (b):

$$A(0^*) \to A(|), \quad A(|) \to A(||), \; \ldots, \; A(n) \to A(n\,|).$$

Puisque $A(0^*)$ est vrai, il s'ensuit de la première implication la vérité de $A(|)$; de la vérité de $A(|)$ et de la seconde implication découle la vérité de $A(||)$, etc. Après $n + 1$ étapes on aboutit à la vérité de $A(n\,|)$ pour tout n de N^*.

Principe de l'induction mathématique (ou de récurrence). L'axiome de l'induction mathématique est la base de la méthode de démonstration par récurrence. La démonstration par récurrence est applicable quand il s'agit de démontrer qu'un prédicat singulaire (à une place) à une variable naturelle libre (condition singulaire) est vrai pour tous les nombres naturels.

THÉORÈME 1.1. *Soit $A(n)$ un prédicat singulaire quelconque sur l'ensemble* N *des nombres naturels satisfaisant aux conditions*: (α) $A(0)$ *est vrai* (0 *satisfait au prédicat* $A(n)$); (β) *pour chaque n de* N, *si $A(n)$ est vrai, $A(n+1)$ l'est aussi. Alors $A(n)$ est vrai pour tout n naturel.*

D é m o n s t r a t i o n. Soit $A = \{n \in N \mid A(n)\}$. En vertu de (α) et (β) les conditions suivantes se vérifient: (a) $0 \in A$, (b) pour tout n de N si $n \in A$ on a aussi $n + 1 \in A$. Selon l'axiome VII il

s'ensuit que $A = \mathbf{N}$. Cette dernière égalité signifie que tout nombre naturel n satisfait à la condition $A(n)$. □

Le théorème 1.1 n'est en fait qu'un autre énoncé de l'axiome de l'induction mathématique et on l'appellera *principe de la récurrence mathématique*. Le principe de la récurrence mathématique peut être écrit sous la forme

$$A(0) \wedge \forall n\, (A(n) \to A(n+1)) \to \forall n A(n)$$

ou bien sous l'aspect

$$\frac{A(0) \wedge \forall n\, (A(n) \to A(n+1))}{\forall n A(n)}.$$

Principales phases de la démonstration par récurrence: 1) on démontre que 0 satisfait à la condition A ; 2) on démontre que pour tout n de $A(n)$ s'ensuit $A(n+1)$. La variable n est nommée *variable sur laquelle s'effectue la récurrence*. La partie de la démonstration qui se lit: « il est vrai que $A(0)$ » est dénommée *départ de la récurrence* ou *base de la récurrence*. La seconde partie de la démonstration qui se lit: « pour tout n de $A(n)$ s'ensuit $A(n+1)$ » est appelée *pas récurrent*. La prémisse « $A(n)$ » est nommée *hypothèse de récurrence*.

Pour démontrer l'affirmation

$$\forall n\, (A(n) \to A(n+1))$$

on prend un entier naturel quelconque en le notant par une lettre arbitraire, par exemple k, et l'on démontre l'implication $A(k) \to A(k+1)$ suivant la voie habituelle: on suppose que $A(k)$ est vrai (hypothèse de récurrence) et l'on montre qu'alors $A(k+1)$ est vrai.

Exercices

1. Démontrer par récurrence sur n que $1 + 2 + \ldots + n = n(n+1)/2$.

2. Démontrer par récurrence sur n que l'ensemble de n éléments possède 2^n sous-ensembles.

3. Soient A et B des ensembles finis composés de m et n éléments respectivement. Démontrer par récurrence sur n que:

(a) le nombre d'applications par récurrence de l'ensemble A dans B est égal à $n(n-1)\ldots(n-m+1)$;

(b) le nombre de toutes les applications possibles de l'ensemble A dans B est égal à n^m.

4. Démontrer que si A est un sous-ensemble de l'ensemble des nombres naturels et que pour un certain n_0 de A est satisfaite la condition: si pour chaque nombre naturel n pour $n \geqslant n_0$ de $n \in A$ il s'ensuit que $n + 1 \in A$, alors chaque nombre naturel $n \geqslant n_0$ appartient à l'ensemble A.

5. Démontrer par récurrence sur n que la composition des fonctions injectives $f_n \circ f_{n-1} \circ \ldots \circ f_1$ est une fonction injective.

6. Démontrer l'affirmation suivante (principe de Dirichlet): s'il faut répartir plus de n objets entre n places une au moins de ces dernières contiendra plus d'un objet.

7. Ecrire les axiomes I-VII du système des nombres naturels en se conformant au langage de la logique des prédicats (en remplaçant l'axiome VII par le principe de récurrence qui lui est équivalent).

8. Donner un exemple d'algèbre du type (2, 2, 0, 0) qui

(a) satisfait aux axiomes II, VII et ne satisfait pas à l'axiome I (du système $\mathscr{N}$);

(b) satisfait aux axiomes I, VII et ne satisfait pas à l'axiome II (du système $\mathscr{N}$);

(c) satisfait aux axiomes I, II et ne satisfait pas à l'axiome VII (du système $\mathscr{N}$).

§ 2. Propriétés de l'addition et de la multiplication des nombres naturels

Propriétés de l'addition. L'addition des nombres naturels vérifie les propriétés suivantes (axiomes):

IV. Pour chaque m de N $m + 0 = m$.

V. Pour tous m et n de N $m + (n + 1) = (m + n) + 1$.

Ces propriétés permettent pour tout nombre naturel fixé m de calculer la somme $m + n$ successivement pour les valeurs de n égales à 0, 1, 2, . . . Par conséquent, ces propriétés permettent d'obtenir la somme $m + n$ pour tous nombres naturels m et n.

Soient, par exemple, $m = 5$ et $n = 3$. En se servant des conditions III, IV et V on est en mesure d'écrire la suite suivante d'égalités:

$5 + 0 = 5$; $5 + 1 = 6$; $5 + 2 = 5 + (1 + 1) = (5 + 1) + + 1 = 6 + 1 = 7$;

$5 + 3 = 5 + (2 + 1) = (5 + 2) + 1 = 7 + 1 = 8$; donc, $5 + + 3 = 8$.

THÉORÈME 2.1. *L'addition des nombres naturels est associative, c'est-à-dire pour tous a, b, c naturels, on a*

(1) $a + (b + c) = (a + b) + c$.

D é m o n s t r a t i o n. Fixons des nombres naturels quelconques a et b. La formule (1) définit alors un prédicat à une variable libre c noté A (c). La démonstration est conduite par récurrence sur la variable naturelle c.

Base de récurrence: A (0) est vrai vu qu'est vraie l'égalité

$a + (b + 0) = (a + b) + 0$.

Pas récurrent. Supposons que pour un certain n naturel A (n) est vrai, c'est-à-dire qu'est vraie la formule

$$a + (b + n) = (a + b) + n$$

et démontrons qu'alors est vrai A ($n + 1$), autrement dit, la formule

$$a + (b + (n + 1)) = (a + b) + (n + 1).$$

En effet,

$$\begin{aligned} a + (b + (n + 1)) &= a + ((b + n) + 1) && \text{(selon l'axiome IV);} \\ &= (a + (b + n)) + 1 && \text{(selon l'axiome IV);} \\ &= ((a + b) + n) + 1 && \text{(suivant l'hypothèse de récurrence);} \\ &= (a + b) + (n + 1) && \text{(selon l'axiome IV).} \end{aligned}$$

Selon le principe de récurrence, le prédicat $A(c)$ est vrai pour tout c naturel. Vu qu'on a fixé lors de la démonstration les valeurs arbitraires de a et b, la formule (1) devient vraie pour tous a et b naturels. □

DÉFINITION. L'algèbre $\langle \mathbf{N}, +, 0 \rangle$ est appelée *monoïde additif des nombres naturels.*

Lemme 2.2. *Pour tous a et b naturels, on a*

(1) $(a + 1) + b = a + (b + 1).$

D é m o n s t r a t i o n. Faisons la démonstration par récurrence sur b. Fixons le nombre naturel arbitraire a. Notons par $B(b)$ le prédicat défini par la formule (1). Convenons que dans ce lemme ainsi que plus loin dans des cas analogues $B(b)$ est également la notation de la formule correspondante.

On voit sans peine que la formule

$B(0)$: $(a + 1) + 0 = a + (0 + 1)$

est vraie. Admettons que pour un certain nombre naturel n est vraie également la formule

$B(n)$: $(a + 1) + n = a + (n + 1),$

et montrons que la formule $B(n + 1)$ est vraie. En effet,

$$\begin{aligned} (a + 1) + (n + 1) &= ((a + 1) + n) + 1 && \text{(selon l'axiome IV);} \\ &= (a + (n + 1)) + 1 && \text{(suivant l'hypothèse de récurrence);} \\ &= a + ((n + 1) + 1) && \text{(selon l'axiome IV).} \end{aligned}$$

Selon le principe de récurrence, la formule $B(b)$ est vraie pour tout nombre naturel b. Vu que lors de la démonstration on a fixé la valeur arbitraire de a, la formule (1) est vraie quels que soient a et b naturels. □

THÉORÈME 2.3. *L'addition des nombres naturels est commutative, c'est-à-dire pour tous a, b naturels, on a*

(1) $a + b = b + a.$

D é m o n s t r a t i o n. Elle est effectuée par récurrence sur b.

Démontrons d'abord que la formule

$A\ (0):\quad a + 0 = 0 + a$

est vraie. Raisonnons par récurrence sur a. La formule est apparemment vraie pour $a = 0$. Ensuite, si pour un certain nombre naturel n

$$n + 0 = 0 + n,$$

il vient alors

$$\begin{aligned}(n + 1) + 0 &= n + (0 + 1) && \text{(suivant le lemme 2.2);}\\ &= (n + 0) + 1 && \text{(suivant l'axiome IV);}\\ &= (0 + n) + 1 && \text{(suivant l'hypothèse de récurrence);}\\ &= 0 + (n + 1) && \text{(suivant l'axiome IV).}\end{aligned}$$

Par conséquent, en vertu du principe de récurrence la formule $A\ (0)$ est vraie pour tout a.

Fixons le choix de a arbitraire. Notons $A\ (b)$ le prédicat défini par la formule (1). Supposons que pour un certain nombre naturel n la formule

$A\ (n):\quad a + n = n + a$

est vraie ; alors

$$\begin{aligned}a + (n + 1) &= (a + n) + 1 && \text{(selon l'axiome IV);}\\ &= (n + a) + 1 && \text{(suivant l'hypothèse de récurrence);}\\ &= n + (a + 1) && \text{(selon l'axiome IV);}\\ &= (n + 1) + a && \text{(selon le lemme 2.2),}\end{aligned}$$

c'est-à-dire que la formule $A\ (n + 1)$ est vraie. Selon le principe de récurrence la formule $A\ (b)$ est vraie pour tout b. Vu que la valeur de a a été fixée de façon quelconque, la formule (1) devient vraie pour tous a et b naturels. □

THÉORÈME 2.4 (RÈGLE DE SIMPLIFICATION DE L'ADDITION). *Pour tous a, b, c naturels, on a*

(1) *si $a + c = b + c$, alors $a = b$.*

D é m o n s t r a t i o n (par récurrence sur c avec choix fixé des valeurs arbitraires a et b). Considérons la formule

$A\ (c):\quad (a + c = b + c) \to (a = b).$

Vu que $a + 0 = a$ et $b + 0 = b$, il est vrai que

$$(a + 0 = b + 0) \to (a = b),$$

c'est-à-dire qu'est vraie la formule $A\ (0)$.

Supposons que pour un certain nombre naturel n

$A(n)$: $(a + n = b + n) \rightarrow (a = b)$,

et montrons qu'alors la formule $A(n + 1)$ est vraie. Selon l'axiome IV

(2) $a + (n + 1) = (a + n) + 1, \quad b + (n + 1) = (b + n) + 1.$

Ensuite, selon l'axiome II

(3) $((a + n) + 1 = (b + n) + 1) \rightarrow (a + n = b + n).$

$A(n)$ et (3) étant vrais il s'ensuit que la formule

(4) $((a + n) + 1 = (b + n) + 1) \rightarrow (a = b)$

est vraie. Sur la base de (2) et (4) on conclut que la formule

$A(n + 1)$: $(a + (n + 1) = b + (n + 1)) \rightarrow (a = b)$

est vraie.

Selon le principe de récurrence la formule $A(c)$ est vraie pour tout c naturel. Vu que le choix de a et b était arbitraire l'affirmation (1) est vraie pour tous a, b, c naturels. □

COROLLAIRE 2.5. *Pour tous a et b naturels, si $b \neq 0$ on a $a \neq a + b$.*

THÉORÈME 2.6. *Pour tout nombre naturel a soit $a = 0$, soit il existe un nombre naturel b tel que $a = b + 1$.*

D é m o n s t r a t i o n. Considérons la formule

$A(a)$: $(a = 0) \vee \exists b\, (a = b + 1)$.

La démonstration de cette formule est faite par récurrence sur a. La formule est apparemment vraie pour $a = 0$. Supposons que pour un certain nombre naturel n la formule

$A(n)$: $(n = 0) \vee \exists b\, (n = b + 1)$

est vraie. Il faut montrer que la formule

$A(n + 1)$: $(n + 1 = 0) \vee \exists b\, (n + 1 = b + 1)$

est vraie. Cette formule est effectivement vraie, car le second membre de la disjonction est une formule vraie (pour $b = n$, $n + 1 = b + 1$). Selon le principe de récurrence la formule $A(a)$ est vraie pour tout a naturel. □

COROLLAIRE 2.7. *Pour tous a et b naturels si $a \neq 0$ ou $b \neq 0$ on a $a + b \neq 0$.*

D é m o n s t r a t i o n. Posons $b \neq 0$. Alors selon le théorème 2.6 il existe un tel c naturel pour lequel $b = c + 1$. En vertu de l'axiome IV

$$a + b = a + (c + 1) = (a + c) + 1.$$

Selon l'axiome I, $(a + c) + 1 \neq 0$; donc, $a + b \neq 0$. □

COROLLAIRE 2.8. *Pour tous a et b naturels si $a + b = 0$, alors $a = 0$ et $b = 0$.*

THÉORÈME 2.9. *Pour tous a et b naturels n'est vraie qu'une et seulement une des trois conditions:*

(α) $a = b$; (β) $a + k = b$ *(pour un certain* $k \in \mathbf{N} \setminus \{0\}$*)*;

(γ) $a = b + m$ *(pour un certain* $m \in \mathbf{N} \setminus \{0\}$*)*.

D é m o n s t r a t i o n. A partir du corollaire 2.5 il s'ensuit que des trois conditions seule une peut être satisfaite. En effet, si les conditions (α) et (β) étaient remplies, on aurait $a = a + k$ et $k \neq 0$, ce qui est impossible en vertu du corollaire 2.5. Si ce sont les conditions (α) et (γ) qui étaient remplies, on aurait $b = b + m$ et $m \neq 0$, ce qui est impossible. Si ce sont les conditions (β) et (γ) qui étaient satisfaites, on aurait $a = a + (k + m)$ et $k + m \neq 0$, ce qui serait également contraire au corollaire 2.5.

Montrons maintenant qu'au moins une des conditions (α), (β), (γ) est satisfaite. Fixons le nombre naturel arbitraire a et notons A (b) la disjonction des conditions (α), (β), (γ). Démontrons par récurrence sur b la vérité de la formule A (b). La formule A (0) est vraie. En effet, si $b = 0$, on a soit $a = 0$, soit $a \neq 0$. Si $a \neq 0$, $a = 0 + m$, où $m = a \neq 0$. Donc, pour $b = 0$ est satisfaite soit la condition (α), soit la condition (γ).

Supposons que pour un certain nombre n est vérifiée la formule

$$A\ (n):\quad (a = n) \vee (a + k = n \text{ pour un certain } k \in \mathbf{N} \setminus \{0\} \vee$$
$$\vee\ (a = n + m \text{ pour un certain } m \in \mathbf{N} \setminus \{0\}),$$

et montrons qu'alors la formule A $(n + 1)$ est vraie. En effet, si $a = n$, alors $a + 1 = b + 1$ et la condition (β) est remplie. Si $a + k = n$, $a + (k + 1) = n + 1$ et c'est la condition (β) qui est remplie. Si, par contre, $a = n + m$, $a + 1 = (n + 1) + m$ et $m \in \mathbf{N} \setminus \{0\}$. Dans ce cas si $m = 1$, $a + 1 = (n + 1) + 1$ et selon l'axiome II $a = n + 1$, la condition (α) est satisfaite. Vu que $m \neq 0$, selon le théorème 2.6 il existe un tel $k \neq 0$ pour lequel $m = k + 1$. Si $m \neq 1$, alors $k \neq 0$ et de l'égalité $a + 1 = (n + 1) + (k + 1) = ((n + 1) + k) + 1$ selon l'axiome II il vient $a = (n + 1) + k$, $k \neq 0$, la condition (γ) est satisfaite. Bref, dans tous les cas la formule A $(n + 1)$ est vraie. Selon le principe de récurrence la formule A (b) est vraie pour tout b naturel. Puisque le choix de a est fixé arbitrairement l'affirmation du théorème est vraie pour tous a et b naturels. □

DÉFINITION. On appelle *différence de deux nombres naturels a et b* un tel nombre naturel k pour lequel $b + k = a$.

Il s'ensuit du théorème 2.9 que la différence de deux nombrec naturels a et b existe au cas où est satisfaite la condition (α) (aves

$k = 0$) ou la condition (γ). Au cas où est satisfaite la condition (β) la différence des deux nombres a et b est inexistante.

On montre sans peine que si la différence des nombres a et b existe, elle est unique. En effet, si $b + k = a$ et $b + m = a$, on a alors $b + k = b + m$, d'où selon la règle de simplification de l'addition il s'ensuit $k = m$.

Le nombre naturel unique constituant la différence des nombres a et b se note $a - b$.

Propriétés de la multiplication. Soit N un ensemble de tous les nombres naturels.

La multiplication des nombres naturels est définie par les conditions suivantes (axiomes):

V. $m \cdot 0 = 0$ pour chaque m de N.

VI. $m\,(n + 1) = m \cdot n + m$ pour tous m, n de N.

Il s'ensuit de ces conditions que

$$m \cdot 1 = m,$$

$$m \cdot 2 = m\,(1 + 1) = m + m,$$

$$m \cdot 3 = m\,(2 + 1) = m \cdot 2 + m = (m + m) + m = m + m + m, \text{ etc.}$$

Donc, une multiplication est une addition répétée du nombre avec lui-même.

THÉORÈME 2.10. LOI DE DISTRIBUTIVITÉ À DROITE DE LA MULTIPLICATION PAR RAPPORT À L'ADDITION). *Pour tous a, b et c naturels, on a*

(1) $(a + b) \cdot c = a \cdot c + b \cdot c$.

Démonstration. Fixons arbitrairement les valeurs de a et b. Notons $A\,(c)$ le prédicat défini dans ce cas par la formule (1). La démonstration est menée par récurrence sur la variable naturelle c. Selon l'axiome V la formule

$$A: (0) \quad (a + b) \cdot 0 = a \cdot 0 + b \cdot 0$$

est vraie.

Supposons que pour un nombre naturel quelconque n la formule

$$A\,(n): \quad (a + b) \cdot n = a \cdot n + b \cdot n$$

est vraie. Il vient alors:

$(a + b) \cdot (n + 1)$	$= (a + b) \cdot n + (a + b)$	(selon l'axiome VI);
	$= (a \cdot n + b \cdot n) + (a + b)$	(suivant l'hypothèse de récurrence);
	$= (a \cdot n + a) + (b \cdot n + b)$	(en vertu de l'associativité et de la commutativité de l'addition);
	$= a\,(n + 1) + b\,(n + 1)$	(selon l'axiome VI),

c'est-à-dire que la formule $A\ (n+1)$ est vraie. Selon le principe de récurrence $A\ (c)$ est vrai pour tout c naturel. Puisqu'on a fixé les valeurs arbitraires de a et b, la formule (1) demeure vraie pour tous a, b et c naturels. □

LEMME 2.11. *Pour tout nombre naturel a on a $1\cdot a = a$.*

D é m o n s t r a t i o n (s'effectue par récurrence sur a). Selon l'axiome V, on a $1\cdot 0 = 0$. Supposons que $1\cdot n = n$ pour un nombre quelconque naturel n. Alors $1\cdot(n+1) = 1\cdot n + 1 = n + 1$, c'est-à-dire $1\cdot(n+1) = n+1$. Selon le principe de récurrence la formule $1\cdot a = a$ est vraie pour tout nombre naturel a. □

THÉORÈME 2.12. *La multiplication des nombres naturels est commutative, c'est-à-dire que pour tous a et b naturels, il vient*

(1) $a\cdot b = b\cdot a.$

D é m o n s t r a t i o n. En recourant à la récurrence sur a montrons que pour tout a la formule

$A\ (0):\quad a\cdot 0 = 0\cdot a$

est vraie. Fixons arbitrairement la valeur de a dans la formule (1). Notons $A\ (b)$ le prédicat défini par l'égalité (1). Supposons que pour un certain nombre naturel n se vérifie la formule

$A\ (n):\quad a\cdot n = n\cdot a.$

Il vient alors

$a\cdot(n+1)$	$= a\cdot n + a$	(selon l'axiome VI);
	$= n\cdot a + a$	(suivant l'hypothèse de récurrence);
	$= n\cdot a + 1\cdot a$	(selon le lemme 2.11);
	$= (n+1)\cdot a$	(en vertu de la distributivité de la multiplication par rapport à l'addition),

c'est-à-dire qu'est vérifiée la formule $A\ (n+1)$. Selon le principe de récurrence $A\ (b)$ est vrai pour tout b naturel. Puisqu'on a fixé la valeur arbitraire de a, la formule (1) est vraie pour tous a et b naturels. □

Des théorèmes 2.10 et 2.12 on déduit le théorème suivant.

THÉORÈME 2.13 (LOI DE DISTRIBUTIVITÉ À GAUCHE DE LA MULTIPLICATION PAR RAPPORT À L'ADDITION). *Pour tous a, b et c naturels se vérifie l'égalité $c\ (a+b) = c\cdot a + c\cdot b$.*

THÉORÈME 2.14. *La multiplication des nombres naturels est associative, c'est-à-dire que pour tous a, b et c naturels on a*

(1) $a\ (bc) = (ab)\ c.$

D é m o n s t r a t i o n (s'effectue par récurrence sur c). Notons $A\ (c)$ le prédicat défini par la formule (1) avec un choix fixé des valeurs de a et de b. Selon l'axiome V, il vient: $b\cdot 0 = 0$ et $(a\cdot b)\cdot 0 =$

$= 0$. Donc, la formule

$A\ (0)\colon\quad a\ (b\cdot 0) = (a\cdot b)\cdot 0$

est vraie. Supposons que pour un certain nombre naturel n se vérifie la formule

$A\ (n)\colon\quad a\ (b\cdot n) = (a\cdot b)\cdot n.$

Il vient alors

$$\begin{aligned} a\cdot(b\cdot(n+1)) &= a\cdot(b\cdot n + b) && \text{(selon l'axiome VI);} \\ &= a\cdot(b\cdot n) + a\cdot b && \text{(selon le théorème 2.13);} \\ &= (a\cdot b)\cdot n + a\cdot b && \text{(suivant l'hypothèse de récurrence);} \\ &= (a\cdot b)\cdot n + (a\cdot b)\cdot 1 && \text{(selon l'axiome V);} \\ &= (a\cdot b)\ (n+1) && \text{(selon le théorème 2.13),} \end{aligned}$$

autrement dit, la formule $A\ (n + 1)$ est vraie. Selon le principe de récurrence la formule $A\ (c)$ est vraie pour tout c naturel. Puisqu'on a fixé les valeurs arbitraires de a, b, la formule (1) est vraie pour tous nombres naturels a, b et c. □

DEFINITION. L'algèbre $\langle N, \cdot, 1\rangle$ est appelée *monoïde multiplicatif des nombres naturels.*

THEOREME 2.15. *Pour tous nombres naturels a et b si $a \neq b$ et $b \neq 0$ on a $ab \neq 0$.*

Démonstration. Supposons que $a \neq 0$ et $b \neq 0$. Selon le théorème 2.6 il existe des nombres naturels m et n pour lesquels $a = m + 1$ et $b = n + 1$. En vertu des axiomes VI et IV, il vient

$$a\cdot b = a\cdot(n+1) = a\cdot n + a = a\cdot n + (m+1) = (a\cdot n + m) + 1.$$

Selon l'axiome I $(a\cdot n + m) + 1 \neq 0$. Donc, $a\cdot b \neq 0$. □

THEOREME 2.16. (RÈGLE DE SIMPLIFICATION DE LA MULTIPLICATION). *Pour tous a, b, c naturels si $ac = bc$ et $c \neq 0$, on a $a = b$.*

Démonstration. Par hypothèse,

(1) $\quad ac = bc, \quad c \neq 0.$

Posons $a \neq b$. Selon le théorème 2.8 soit il existe un k tel que $a + k = b$ et $k \neq 0$, soit il existe un m tel que $a = b + m$ et $m \neq 0$. Dans le premier cas $bc = ac + kc$ et en vertu de (1) $bc = bc + kc$, ce qui (selon le corollaire 2.5) est impossible, car $k \neq 0$, $c \neq 0$ et (selon le théorème 2.15) $kc \neq 0$. Dans le second cas un raisonnement analogue montre qu'avec l'hypothèse $a \neq b$, on aboutit à une contradiction. □

Exercices

1. Démontrer les formules:

(a) $1 + 3 + 5 + \ldots + (2n + 1) = (n + 1)^2$;

(b) $1^2 + 2^2 + \ldots + n^2 = n(n + 1)(2n + 1)/6$;

(c) $1 \cdot 2 + 2 \cdot 3 + \ldots + (n - 1)n = (n - 1)n(n + 1)/3$ pour $n > 1$;

(d) $(1 + 2 + \ldots + n)^2 = 1^3 + 2^3 + \ldots + n^3$;

(e) $1^2 + 3^2 + \ldots + (2n - 1)^2 = n(2n - 1)(2n + 1)/3$.

2. Démontrer que le nombre C_n^k des sous-ensembles comportant k éléments de l'ensemble de n éléments ($1 \leqslant k \leqslant n$) peut être exprimé par la formule

$$C_n^k = \frac{n(n-1)\ldots(n-k+1)}{1 \cdot 2 \ldots k}.$$

3. Démontrer que $C_{n+1}^k = C_n^k + C_n^{k-1}$ pour $n \geqslant k > 1$.

4. Démontrer que pour tout n naturel ($n > 1$)

$$(x + 1)^n = x^n + C_n^1 x^{n-1} + C_n^2 x^{n-2} + \ldots + C_n^n.$$

5. Démontrer que

$$1 + C_n^1 + C_n^2 + \ldots + C_n^n = 2^n.$$

6. Démontrer que $\sum\limits_{k=0}^{n} (C_n^k)^2 = C_{2n}^n$.

7. Démontrer que pour tous nombres naturels a, b, c et d la somme $a + b + c + d$ est indépendante de l'ordre des termes.

§ 3. Relation d'ordre sur un ensemble des nombres naturels

Relation d'ordre. Considérons la relation d'ordre sur un ensemble des nombres naturels.

Définition. Si pour des nombres naturels a et b il existe un nombre naturel k tel que $a + k = b$ et $k \neq 0$, on dit alors que « a est inférieur à b » et l'on écrit $a < b$. On dit que « a est inférieur ou égal à b » et l'on écrit $a \leqslant b$ si $a < b$ ou $a = b$.

La relation inverse de la relation $<$ est notée par le symbole $>$. Donc, $a > b$ si et seulement si $b < a$. Si $a > b$ ou $a = b$ on dit que « a est supérieur ou égal à b » et l'on écrit $a \geqslant b$. La relation $\geqslant$ est *l'inverse* de la relation $\leqslant$.

Théorème 3.1. *Pour tous nombres naturels a et b, il vient:*

(1) *si $a < b$, alors $a + 1 \leqslant b$;*

(2) $0 \leqslant a$;

(3) *si $a \neq 0$, alors $0 < a$;*

(4) *$a \leqslant b$ si et seulement s'il existe un nombre naturel k tel que $a + k = b$.*

La démonstration du théorème se déduit facilement des définitions des relations $<$ et $\leqslant$; on laisse au lecteur le soin de l'esquisser.

DÉFINITION. Le système algébrique $\langle \mathrm{N}, +, \cdot, < \rangle$ est appelé *système ordonné des nombres naturels.*

THÉORÈME 3.2 (LOI DE LA TRICHOTOMIE DE $<$). *Pour tous nombres naturels a et b une et seulement une des trois conditions $a < b$, $a = b$, $a > b$ est remplie.*

Ce théorème découle directement de la définition de la relation $<$ et du théorème 2.9.

COROLLAIRE 3.3. *Pour tous nombres naturels a et b on a:*

(1) $a \leqslant a$ *(réflexivité de $\leqslant$);*
(2) *soit $a \leqslant b$, soit $b \leqslant a$ (rapport de connexion de $\leqslant$);*
(3) *si $a \leqslant b$ et $b \leqslant a$, alors $a = b$ (antisymétrie de $\leqslant$).*

THÉORÈME 3.4. *La relation binaire $<$ sur un ensemble des nombres naturels est transitive, c'est-à-dire que pour tous nombres naturels a, b et c si $a < b$ et $b < c$, on a $a < c$.*

Démonstration. Supposons que $a < b$ et $b < c$. Il existe alors des nombres naturels k et m satisfaisant aux conditions:

(1) $a + k = b, \quad b + m = c;$

(2) $k \neq 0, \quad m \neq 0.$

En vertu de (1) $a + (k + m) = c$, de plus, en vertu de (2) et du corollaire 2.7, $k + m \neq 0$; donc $a < c$. □

COROLLAIRE 3.5. *La relation $<$ sur un ensemble des nombres naturels est une relation d'ordre total strict. Le système $\langle \mathrm{N}, < \rangle$ est un ensemble totalement ordonné.*

COROLLAIRE 3.6. *Pour tous nombres naturels a, b et c, on a:*

(1) *si $a \leqslant b$ et $b < c$, alors $a < c$;*

(2) *si $a < b$ et $b \leqslant c$, alors $a < c$;*

(3) *si $a \leqslant b$ et $b \leqslant c$, alors $a \leqslant c$.*

COROLLAIRE 3.7. *La relation binaire $\leqslant$ sur un ensemble des nombres naturels est une relation d'ordre total non strict.*

THÉORÈME 3.8. *La relation $<$ est monotone par rapport à l'addition et à la multiplication, c'est-à-dire que pour tous nombres naturels a, b et c, on a:*

(1) *$a < b$ si et seulement si $a + c < b + c$;*

(2) *si $a < b$ et $c \neq 0$, alors $ac < bc$.*

Démonstration. La condition $a + c < b + c$ est équipotente à la condition $a + c + k = b + c$ et $k \neq 0$, k étant un certain nombre naturel qui suivant la règle de simplification est équipotent à la condition $a + k = b$ et $k \neq 0$ pour un certain k naturel, autrement dit, à la condition $a < b$.

Supposons que $a < b$ et $c \neq 0$. Il existe un tel nombre naturel k pour lequel $a + k = b$, $k \neq 0$. En multipliant les deux membres de

l'égalité par c, on obtient $ac + kc = bc$. Selon le théorème 2.15, $kc \neq 0$, puisque $k \neq 0$ et $c \neq 0$; donc, $ac < bc$. □

COROLLAIRE 3.9. *La relation $\leqslant$ est monotone par rapport à l'addition et à la multiplication, c'est-à-dire que pour tous a, b et c naturels on a:*

(1) *$a \leqslant b$ si et seulement si $a + c \leqslant b + c$;*

(2) *si $a \leqslant b$, alors $ac \leqslant bc$.*

THÉORÈME 3.10. *Pour tous nombres naturels a, b et c de $ac < bc$ s'ensuit $a < b$.*

Démonstration. Selon le corollaire 3.9 pour tous a, b, c naturels

si $b \leqslant a$, alors $bc \leqslant ac$. De la loi de contraposition s'ensuit l'affirmation:

si $ac < bc$, alors $a < b$. □

Ordre total d'un ensemble des nombres naturels.

THÉORÈME 3.11. *Le système $\langle \mathrm{N}, < \rangle$ est un ensemble bien ordonné.*

Démonstration. Selon le corollaire 3.7 le système $\langle \mathrm{N}, < \rangle$ est un ensemble totalement ordonné. On doit démontrer que tout sous-ensemble non vide de l'ensemble N des nombres naturels possède le plus petit élément. Supposons qu'il existe un sous-ensemble non vide A de l'ensemble N ne possédant pas de plus petit élément. Démontrons par récurrence sur la variable naturelle b que pour tout b se vérifie la formule

$$A\,(b):\quad a \in A \rightarrow b \leqslant a.$$

Apparemment, la formule est vraie pour $b = 0$, c'est-à-dire que

$$A\,(0):\quad a \in A \rightarrow 0 \leqslant a.$$

Posons que pour tout a et un certain nombre naturel n se vérifie la formule

$$A\,(n):\quad a \in A \rightarrow n \leqslant a.$$

Dans ce cas $n \notin A$, car dans le cas contraire n serait le plus petit élément de l'ensemble A; donc, $a \in A \rightarrow n < a$. Vu que, selon le théorème 3.1, de $n < a$ s'ensuit $n + 1 \leqslant a$, il vient

$$A\,(n+1):\quad a \in A \rightarrow n + 1 \leqslant a.$$

Par conséquent, pour tout n naturel se vérifie l'implication $A\,(n) \rightarrow A\,(n + 1)$. On a ainsi démontré que la formule $A\,(b)$ est vraie pour tout b naturel.

Par hypothèse, l'ensemble A n'est pas vide et, par suite, il existe un élément $m \in A$. En posant dans la formule $A\,(b)$ $a = m$ et $b = m + 1$, on obtient $m \in A \rightarrow m + 1 \leqslant m$. De là, puisque $m \in A$, il vient que $m + 1 \leqslant m$, c'est-à-dire que l'on aboutit à une contradiction. □

THÉORÈME 3.12. *Soit A un sous-ensemble de l'ensemble* **N** *de tous les nombres naturels. Si pour chaque nombre naturel n se vérifie la condition*

(1) $(\forall m < n)\,(m \in A) \rightarrow n \in A$,

alors $A = \mathbf{N}$.

Démonstration. Posons que $A \neq \mathbf{N}$. Dans ce cas l'ensemble $\mathbf{N} \setminus A$ n'est pas vide et (selon le théorème 3.11) possède un plus petit élément; il existe donc un nombre naturel k satisfaisant aux conditions:

(2) $k \in \mathbf{N} \setminus A$;

(3) $(\forall m < k)\,(m \in A)$.

En vertu de la condition (1) on a l'implication

(4) $(\forall m < k)\,(m \in A) \rightarrow k \in A$.

D'après la règle de séparation il s'ensuit de (3) et (4) que $k \in A$, ce qui, en vertu de (2), est impossible. □

THÉORÈME 3.13. *Soit $A(x)$ un prédicat singulaire quelconque sur un ensemble* **N** *des nombres naturels. Si pour tout nombre naturel n*

$$(\forall m < n)\, A(m) \rightarrow A(n),$$

alors on a $A(x)$ pour tout x naturel.

La démonstration du théorème 3.13 se déduit sans peine du théorème 3.12; le soin de l'esquisser est laissé au lecteur.

Exercices

1. Montrer que pour tous nombres naturels a, b, c et d:
(a) si $a < b$ et $c < d$, alors $a + c < b + d$;
(b) si $a < b$ et $c < d$, alors $ac < bd$.

2. Démontrer que pour tous nombres naturels a_i, b_i si $a_1 < b_1$, $a_2 < b_2$, ..., $a_n < b_n$, on a $a_1a_2 \ldots a_n < b_1b_2 \ldots b_n$.

3. Démontrer que pour tous nombres naturels a_i, b_i si $0 < a_1 \leqslant b_1$, $0 < a_2 \leqslant b_2$, ..., $0 < a_n \leqslant b_n$, on a

(1) $a_1a_2 \ldots a_n \leqslant b_1b_2 \ldots b_n$,

de plus, l'égalité dans (1) a lieu si et seulement si $a_1 = b_1$, ..., $a_n = b_n$.

4. Montrer que pour tous nombres naturels a, b et c se vérifie l'inégalité $ab + bc + ca \leqslant a^2 + b^2 + c^2$.

5. Démontrer que pour tous nombres naturels a, b et $n > 1$ se vérifie l'inégalité $(a + b)^n \leqslant 2^{n-1}(a^n + b^n)$.

6. Démontrer les inégalités:
(a) $n^2 < 2^n$ pour tout n naturel si $n \geqslant 4$;
(b) $2^n < n!$ pour tout n naturel si $n \geqslant 4$;
(c) $n! < \left(\frac{n+1}{2}\right)^n$ pour tout n natirel si $n > 1$.

7. Démontrer par récurrence sur n l'inégalité de Bernoulli $(1 + a)^n \geqslant 1 + na$, où a est un nombre réel quelconque supérieur à (-1).

§ 4. Anneau des entiers

Groupe additif des entiers. Soit $\mathcal{N} = \langle N, +, \cdot, 0, 1\rangle$ un système des nombres naturels. L'opération de soustraction n'est pas toujours possible dans $\mathcal{N}$, autrement dit, pour les nombres naturels donnés m et n l'équation $m + x = n$ n'a pas toujours de solution dans N par rapport à x. C'est seulement quand $m \leqslant n$ que l'équation possède une solution dans N et de plus unique (selon le théorème 4.2.9); cette solution est nommée *différence entre les nombres n et m* et se note $n - m$.

Il s'agit de démontrer qu'il existe un groupe additif abélien $\mathfrak{Z}$ satisfaisant aux conditions:

(1) l'ensemble N est inclus dans $|\mathfrak{Z}|$ et l'addition dans le groupe $\mathfrak{Z}$ est un prolongement de l'addition dans $\mathcal{N}$;

(2) l'opération de soustraction dans $\mathfrak{Z}$ est toujours possible et tout élément du groupe $\mathfrak{Z}$ peut se représenter sous forme de différence des nombres naturels.

Un tel groupe sera appelé *groupe additif des entiers.*

THÉORÈME 4.1. *Soit $\mathcal{N} = \langle N, \boldsymbol{+}, \cdot, 0, 1\rangle$ un système des nombres naturels. Il existe un groupe abélien $\mathfrak{Z} = \langle Z, +, -\rangle$ qui satisfait aux conditions:*

(α) $N \subset Z$ *et la somme de deux nombres naturels quelconques m et n du groupe $\mathfrak{Z}$ coïncide avec la somme de ces éléments de $\mathcal{N}$, c'est-à-dire que* $m + n = m \boldsymbol{+} n$;

(β) *pour tout élément a de Z il existe des nombres naturels n et m tels que* $n + a = m$.

Démonstration. Considérons l'ensemble $N \times N$ de couples des nombres naturels. Définissons sur cet ensemble la relation binaire $\sim$ de la façon suivante:

(1) $\langle m, n\rangle \sim \langle r, s\rangle$ si et seulement si $m \boldsymbol{+} s = r \boldsymbol{+} n$.

Une vérification directe montre que la relation $\sim$ est une relation d'équivalence sur l'ensemble $N \times N$.

Définissons sur l'ensemble $N \times N$ l'opération binaire $\oplus$ (addition) et l'opération singulaire $\ominus$ au moyen des formules

(2) $\langle m, n\rangle \oplus \langle p, q\rangle = \langle m \boldsymbol{+} p, n \boldsymbol{+} q\rangle$;

(3) $\ominus \langle m, n\rangle = \langle n, m\rangle$.

L'addition des couples est commutative et associative. Cela découle directement de la commutativité et de l'associativité de l'addition des nombres naturels.

Une vérification directe montre que l'équivalence $\sim$ est une congruence par rapport aux opérations $\oplus$ et $\ominus$, c'est-à-dire que de

$$\langle m, n\rangle \sim \langle k, l\rangle \text{ et } \langle p, q\rangle \sim \langle r, s\rangle$$

s'ensuit

$$\langle m, n\rangle \oplus \langle p, q\rangle \sim \langle k, l\rangle \oplus \langle r, s\rangle$$

et de $\langle m, n\rangle \sim \langle k, l\rangle$ découle

$$\ominus \langle m, n\rangle \sim \ominus \langle k, l\rangle.$$

Notons $[m, n]$ la classe d'équivalence comportant le couple $\langle m, n\rangle$. Selon le théorème 3.1 les opérations $\oplus$, $\ominus$ (voir formules (2) et (3)) induisent sur l'ensemble quotient $Z_1 = \mathbf{N} \times \mathbf{N}/\sim$ les opérations $+$, $-$:

(4) $[m, n] + [p, q] = [m + p, n + q]$;

(5) $-[m, n] = [n, m]$.

En vertu de (1), il vient

(6) $[m, n] = [r, s]$

si et seulement si $m + s = r + n$.

L'algèbre $\mathfrak{Z}_1 = \langle Z_1, +, -\rangle$ est un groupe abélien. En effet, une vérification directe à l'aide des formules (4)-(6) montre que l'addition dans Z_1 est commutative et associative. L'élément $[0, 0]$ est un élément neutre par rapport à l'addition dans $\mathfrak{Z}_1$, vu qu'en vertu de (4) $[m, n] + [0, 0] = [m, n]$. L'élément $-[m, n]$ est opposé à l'élément $[m, n]$, car en vertu de (4)-(6)

$$[m, n] + (-[m, n]) = [m, n] + [n, m] =$$
$$= [m + n, m + n] = [0, 0].$$

Ce qui signifie que l'algèbre $\mathfrak{Z}_1$ est un groupe abélien.

Considérons l'ensemble

$$\mathbf{N}^* = \{[0, k] \mid k \in \mathbf{N} \setminus \{0\}\}.$$

La réunion des ensembles $\mathbf{N}$ et $\mathbf{N}^*$ sera notée $\mathbf{Z}$:

$$\mathbf{Z} = \mathbf{N} \cup \mathbf{N}^*.$$

Définissons l'application h de l'ensemble Z_1 sur $\mathbf{Z}$ de la façon suivante:

$$h([m + k, m]) = k \text{ pour tout } k \text{ de } \mathbf{N};$$

$$h([n, n + k]) = [n, n + k] \text{ pour tout } k \text{ de } \mathbf{N} \setminus \{0\}.$$

On constate sans peine que h est une application injective de l'ensemble Z_1 sur $\mathbf{Z}$. Il existe donc une application inverse h^{-1}, application injective de l'ensemble $\mathbf{Z}$ sur Z_1 qui satisfait aux conditions

$$h \circ h^{-1} = i_{\mathbf{Z}}, \quad h^{-1} \circ h = i_{Z_1},$$

où $i_{\mathbf{Z}}$ et i_{Z_1} sont des applications identiques de $\mathbf{Z}$ et Z_1 respectivement.

Définissons l'addition dans **Z** pour tous a, b de **Z** à l'aide de la formule

(I) $\quad a + b = h\,(h^{-1}\,(a) + h^{-1}\,(b)),$

quant à l'opération singulaire, on la définira par la formule

(II) $\quad -a = h\,(-h^{-1}\,(a)).$

Des formules (I) et (II) se déduisent les formules

(III) $\quad h^{-1}\,(a + b) = h^{-1}\,(a) + h^{-1}\,(b),$

(IV) $\quad h^{-1}\,(-a) = -h^{-1}\,(a).$

Considérons l'algèbre $\mathfrak{Z} = \langle \mathbf{Z}, +, - \rangle$. En vertu de (III) et (IV) l'algèbre $\mathfrak{Z}$ est isomorphe au groupe abélien $\mathfrak{Z}_1$. Il s'ensuit que l'algèbre $\mathfrak{Z}$ est un groupe abélien. En effet, l'addition dans $\mathfrak{Z}$ est commutative, car, en vertu de (I) et de la commutativité de l'addition dans $\mathfrak{Z}_1$, il vient

$$a + b = h\,(h^{-1}\,(a) + h^{-1}\,(b)) = h\,(h^{-1}\,(b) + h^{-1}\,(a)) = b + a.$$

L'addition dans $\mathfrak{Z}$ est associative, vu qu'en vertu de (I) et (II), il vient

$$a + (b + c) = h\,(h^{-1}\,(a) + h^{-1}\,(b + c)) = h\,(h^{-1}\,(a) +$$
$$+ h^{-1}\,(b) + h^{-1}\,(c)) = h\,(h^{-1}\,(a + b) + h^{-1}\,(c)) = (a + b) + c.$$

Le nombre naturel 0 est un élément neutre par rapport à l'addition dans $\mathfrak{Z}$, car pour tout a de **Z** on a

$$a + 0 = h\,(h^{-1}\,(a) + h^{-1}\,(0)) = h\,(h^{-1}\,(a) + [0, 0]) =$$
$$= h\,(h^{-1}\,(a)) = a.$$

Pour tout a de **Z** se vérifie l'égalité $a + (-a) = 0$, vu que

$$a + (-a) = h\,(h^{-1}\,(a) + h^{-1}\,(-a)) =$$
$$= h\,(h^{-1}\,(a) + (-h^{-1}\,(a)) = h\,([0, 0]) = 0.$$

Donc, l'algèbre $\mathfrak{Z}$ est un groupe abélien.

Montrons que la condition (α) est vraie. En effet, en vertu de (I) pour tous m, n de **N**, on a

$$m + n = h\,(h^{-1}\,(m) + h^{-1}\,(n)) = h\,([m, 0] + [n, 0]) =$$
$$= h\,([m + n, 0]) = m + n,$$

autrement dit, l'addition dans $\mathfrak{Z}$ prolonge l'addition dans $\mathcal{N}$.

Montrons que la condition (β) est vraie. Soient a un élément quelconque de **Z** et $h^{-1}\,(a) = [m, n]$; dans ce cas

$$n + a = h\,(h^{-1}\,(n) + h^{-1}\,(a)) =$$
$$= h\,([n, 0] + [m, n]) =$$
$$= h\,([n + m, n]) = m, \text{ c'est-à-dire que } n + a = m.$$

Par conséquent, tout élément de $\mathbf{Z}$ peut se représenter sous forme d'une différence des nombres naturels: $a = m - n$.

Bref, on a établi que l'algèbre $\mathfrak{Z} = \langle \mathbf{Z}, +, - \rangle$ est un groupe abélien satisfaisant aux conditions (α) et (β). □

Définition. On appelle *groupe additif des entiers* le groupe abélien $\mathfrak{Z} = \langle \mathbf{Z}, +, - \rangle$ qui satisfait aux conditions (α) et (β) du théorème 4.1.

Multiplication naturelle dans un groupe additif des entiers. Soit $\mathfrak{Z}_+ = \langle \mathbf{Z}, +, - \rangle$ un groupe additif des entiers. Selon le théorème 4.1, $\mathbf{N} \subset \mathbf{Z}$ et tout élément de $\mathbf{Z}$ peut être représenté sous forme d'une différence des nombres naturels; donc,

$$\mathbf{Z} = \{m - n \mid m, \quad n \in \mathbf{N}\}.$$

Définissons la multiplication dans le groupe $\mathfrak{Z}_+$ de la façon suivante: pour tous éléments $m - n$ et $p - q$ de $\mathbf{Z}$ on pose

$$(1) \quad (m - n)\cdot(p - q) = (mp + nq) - (mq + np),$$

où $m, n, p, q \in \mathbf{N}$ et mp, nq, mq, np sont des produits des nombres naturels dans le système $\mathcal{N}$.

Représentons tout élément de $\mathbf{Z}$ sous forme d'une différence des nombres naturels de façon non univoque. Il nous faut donc vérifier que le produit des entiers défini par la formule (1) est indépendant de leur représentation sous forme d'une différence des nombres naturels. Montrons que pour tout élément $p - q$ de l'ensemble $\mathbf{Z}$ de l'égalité

$$(2) \quad m - n = m' - n' \qquad (m, n, m', n' \in N)$$

s'ensuit l'égalité

$$(3) \quad (m' - n')\cdot(p - q) = (m - n)\cdot(p - q).$$

En effet, par définition (1),

$$(m' - n')(p - q) = (m'p + n'q) - (m'q + n'p).$$

Selon (1) est (4) il suffit de vérifier que

$$(4) \quad (mp + nq) + (m'q + n'p) = (m'p + n'q) + (mq + np),$$

ou

$$(5) \quad (m + n')\,p + (n + m')\,q = (m' + n)\,p + (n' + m)\,q.$$

En raison de (2) $m + n' = m' + n$. Donc, les égalités (5), (4) et (3) sont vraies.

Une vérification directe de nature aussi simple montre que pour tous éléments $m - n$ et $p - q$ de l'ensemble $\mathbf{Z}$ des égalités

$$m - n = m' - n' \quad \text{et} \quad p - q = p' - q'$$

s'ensuit l'égalité

$$(m' - n')\cdot(p' - q') = (m - n)(p - q).$$

Bref, il a été établi qu'une multiplication dans le groupe $\mathfrak{Z}_+$ définie par la formule (1) est indépendante du mode de représentation des facteurs sous forme de différence des nombres naturels.

DEFINITION. La multiplication dans un groupe additif des entiers $\mathfrak{Z}_+$ définie par la formule (1) est nommée *multiplication naturelle.*

Anneau des entiers. Donnons d'abord la définition.

DEFINITION. L'anneau $\mathcal{K}$ est appelé *anneau des entiers* si le groupe additif de l'anneau $\mathcal{K}$ est un groupe additif des entiers et la multiplication dans l'anneau $\mathcal{K}$ est commutative et prolonge la multiplication des nombres naturels (dans le système $\mathcal{N}$ des nombres naturels).

THÉORÈME 4.2. *Soient* $\langle \mathbf{Z}, +, - \rangle$ *un groupe additif des entiers,* $\cdot$ *une multiplication naturelle dans ce groupe et* 1 *l'unité du système N des nombres naturels. Dans ce cas l'algèbre* $\mathfrak{Z} = \langle \mathbf{Z}, +, -, \cdot, 1 \rangle$ *est un anneau des entiers.*

D é m o n s t r a t i o n. Montrons que l'algèbre $\mathfrak{Z}$ est un anneau commutatif. Par hypothèse, l'algèbre $\langle \mathbf{Z}, +, - \rangle$, groupe additif de l'anneau, est un groupe abélien, vu que c'est un groupe additif des entiers.

Soient a, b, c des éléments arbitraires de l'ensemble $\mathbf{Z}$. Selon le théorème 4.1 on peut les représenter sous forme de différence des nombres naturels. Posons

(1) $\quad a = m - n, \quad b = p - q, \quad c = r - s \quad (m, n, p, q, r, s \in N).$

Une multiplication naturelle dans $\mathbf{Z}$ se définit par la formule

(2) $\quad a \cdot b = (m - n) \cdot (p - q) = (mp + nq) - (mq + np).$

Une multiplication naturelle est commutative, car

$$b \cdot a = (p - q) \cdot (m - n) = (pm + qn) - (pn + qm),$$

de même sont commutatives l'addition et la multiplication des nombres naturels.

Une multiplication naturelle est associative. En effet, en vertu de (1) et (2), il vient:

$$\begin{aligned} a \cdot (b \cdot c) &= (m - n) [(p - q)(r - s)] = \\ &= (m - n) [(pr + qs) - (ps + qr)] = \\ &= (mpr + mqs + nps + nqr) - \\ &- (mps + mqr + npr + nqs); \\ (a \cdot b) \cdot c &= [(m - n)(p - q)] (r - s) = \\ &= [(mp + nq) - (mq + np)] (r - s) = \\ &= (mpr + nqr + mqs + nps) - \\ &- (mps + nqs + mqr + npr). \end{aligned}$$

Par conséquent, en vertu de la commutativité de l'addition des nombres naturels $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

L'élément 1 est un élément neutre par rapport à la multiplication naturelle. En effet, pour tout a de **Z**, il vient

$$a\cdot 1 = (m - n)(1 - 0) = m\cdot 1 - n\cdot 1 = m - n = a.$$

Donc, l'algèbre $\langle \mathbf{Z}, \cdot, 1\rangle$ est un monoïde commutatif.

La multiplication naturelle est distributive par rapport à l'addition. En effet,

$$(a + b)\cdot c = [(m + p) - (n + q)]\,(r - s) =$$
$$= (mr + pr + ns + qs) - (ms + ps + nr + qr);$$
$$ac + bc = [(mr + ns) - (ms + nr)] + [(pr + qs) - (ps + qr)] =$$
$$= (mr + ns + pr + qs) - (ms + nr + ps + qr).$$

Par conséquent, $(a + b)\cdot c = a\cdot c + b\cdot c$. Vu que la multiplication naturelle est également commutative, on a de même l'égalité $c\,(a + b) = ca + cb$.

Bref, on a établi que l'algèbre $\mathfrak{Z}$ est un anneau commutatif.

La multiplication naturelle prolonge la multiplication des nombres naturels dans le système $\mathcal{N} = \langle \mathbf{N}, +, \cdot, 0, 1\rangle$. En effet, pour m et n de **N**, on a

$$m\cdot n = (m - 0)(n - 0) = (m\cdot n + 0\cdot 0) - (m\cdot 0 + n\cdot 0) = m\cdot n.$$

De plus, par hypothèse, le groupe additif de l'anneau $\mathfrak{Z}$ est un groupe additif des entiers. Par conséquent, l'anneau $\mathfrak{Z}$ est un anneau des entiers. □

DÉFINITION. Si pour deux entiers a et b il existe un nombre naturel k tel que $a + k = b$ et $k \neq 0$, on dit alors que « a est inférieur à b » et l'on écrit $a < b$. On dit que « a est inférieur ou égal à b » et l'on écrit $a \leqslant b$ si $a < b$ ou $a = b$.

La relation inverse de $<$ est notée par le symbole $>$. Donc, $a > b$ si et seulement si $b < a$.

THÉORÈME 4.3. *Soit* $\mathfrak{Z} = \langle \mathbf{Z}, +, -, \cdot, 1\rangle$ *un anneau des entiers. Il vient alors*

(1) *pour tous entiers a et b est satisfaite une et seulement une des trois conditions*: $a < b$, $a = b$, $b < a$;

(2) *pour tout entier a est satisfaite une et seulement une des trois conditions*: $a < 0$, $a = 0$, $0 < a$;

(3) *la relation* $<$ *est monotone par rapport à l'addition, autrement dit, pour tous entiers a, b et c*

$$a < b \text{ si et seulement si } a + c < b + c;$$

(4) *la relation* $<$ *est monotone par rapport à la multiplication, autrement dit, pour tous entiers a, b et c*

$$\text{si } a < b \text{ et } c > 0, \text{ on a } ac < bc.$$

La démonstration de ce théorème est laissée au soin du lecteur.

Théorème de division avec reste. Soient a un entier et b un nombre naturel différent de zéro. Diviser a par b avec reste c'est le représenter sous la forme $a = bq + r$, où $0 \leqslant r < b$, q et r étant des entiers. q est dans ce cas nommé *quotient entier*, tandis que r est le *reste* de la division de a par b.

Une division avec reste est toujours possible, tandis que le quotient incomplet (entier) et le reste sont définis de façon univoque par le nombre divisé (dividende) et le diviseur comme le montre le théorème suivant.

THÉORÈME 4.4. *Pour tous entiers a, b pour $b > 0$ il n'existe qu'un seul couple d'entiers q et r satisfaisant aux conditions*:

(1) $a = bq + r$ *et* $0 \leqslant r < b$.

Démonstration. Démontrons qu'il existe au moins un couple de nombres q, r satisfaisant aux conditions (1). Considérons d'abord le cas où a est un nombre naturel. Fixons b et démontrons par récurrence sur a que

(2) *il existe un couple d'entiers q, r satisfaisant à* (1).

Pour $a = 0$ l'affirmation (2) est vraie, car $0 = b \cdot 0 + 0$. Admettons que (2) est vraie pour $a = n$, c'est-à-dire qu'il existe des entiers q, r tels que

(3) $n = bq + r$ et $0 \leqslant r < b$,

et démontrons qu'elle est vraie pour $a = n + 1$. Il s'ensuit de (3) que $n + 1 = bq + (r + 1)$ et $0 < r + 1 \leqslant b$. Si $r + 1 < b$ le couple de nombres q, $r + 1$ est justement le couple cherché. Si, par contre, $r + 1 = b$, alors $n + 1 = b(q + 1)$ et le couple de nombres $q + 1$, 0 est le couple cherché.

Considérons maintenant le cas où $a < 0$; on a alors $-a > 0$. En vertu de la démonstration faite plus haut, il existe pour le couple de nombres $-a$, b des entiers q', r' tels que $-a = bq' + r'$ et $0 \leqslant r' < b$. Si $r' = 0$, $a = (b - q') + 0$. Si, par contre, $r' > 0$, alors $a = b(-q' - 1) + (b - r')$ et $0 < b - r' < b$.

En posant $q = -q' - 1$ et $r = b - r'$, il vient

$$a = bq + r \quad \text{et} \quad 0 < r < b.$$

Bref, on a démontré que pour tous entiers a, b pour $b > 0$, il existe au moins un couple d'entiers q, r satisfaisant aux conditions (1).

Il reste à démontrer que le couple d'entiers satisfaisant aux conditions (1) est unique. Supposons que pour l'entier a on a deux représentations:

(4) $a = bq + r$, $\quad 0 \leqslant r < b$;

(5) $a = bq_1 + r_1$, $\quad 0 \leqslant r_1 < b$.

Posons que $r \neq r_1$. Alors, $r > r_1$ ou $r_1 > r$. Si $r > r_1$, en vertu de (4) et (5), on a

(6) $0 < r - r_1 < b$;

(7) $r - r_1 = b(q_1 - q)$.

De (6) et (7) il s'ensuit que $q_1 - q > 0$ et, par suite, $q_1 - q \geqslant 1$. De là, en vertu de (7), découle l'inégalité $r - r_1 \geqslant b$ qui contredit (6). On se convainc de façon analogue qu'est également impossible le cas de $r_1 > r$. Par conséquent, $r = r_1$ et, en vertu de (4), (5), $b(q - q_1) = 0$. Comme $b \neq 0$, on a: $q - q_1 = 0$ et $q = q_1$. □

Relation de divisibilité dans un anneau des entiers. Etudions les plus simples des propriétés de la divisibilité dans un anneau des entiers.

Définition. Soient a et b des entiers. On dit que b divise a si $a = bq$ pour un certain entier q. Au lieu de « b divise a » on dit aussi que a est divisible par b, ou que a est un multiple de b, et l'on écrit $b \mid a$ ou $a \vdots b$. Dans le cas contraire on dit que *a ne se divise pas par b, a n'est pas un multiple de b, b ne divise pas a, b n'est pas un diviseur de a* et l'on écrit $b \nmid a$.

Théorème 4.5. *Soient a, b, c, d, m, n des entiers quelconques. On a alors*

(1) $a \mid a$;

(2) $a \mid 0$;

(3) *si* $0 \mid a$, *alors* $a = 0$;

(4) $\pm 1 \mid a$;

(5) *si* $a \mid b$ *et* $b \mid c$, *alors* $a \mid c$, *c'est-à-dire que la relation de divisibilité est transitive*;

(6) *si* $c \mid a$, *alors* $c \mid ab$;

(7) *si* $c \mid a$ *et* $c \mid b$, *alors* $c \mid (a \pm b)$;

(8) *si* $b \mid a$, *alors* $bc \mid ac$;

(9) *si* $c \neq 0$, *alors de* $bc \mid ac$ *s'ensuit* $b \mid a$;

(10) *si* $a \mid c$ *et* $b \mid d$, *alors* $ab \mid cd$;

(11) *si* $a \mid b$ *et* $a \mid c$, *alors* $a \mid (mb + nc)$.

Les propriétés (1)-(11) de la relation de divisibilité se déduisent facilement de la définition de la divisibilité et des propriétés de l'anneau $\mathbb{Z}$. La démonstration est laissée au soin du lecteur.

Lemme 4.6. *Si le produit ab des nombres naturels est égal à l'unité, on a alors $a = b = 1$.*

Démonstration. De l'hypothèse $ab = 1$ il s'ensuit que a et b sont différents de zéro. Selon le théorème 2.6 ils peuvent être

représentés sous forme de $a = c + 1$, $b = d + 1$. Donc, $ab = cd + c + d + 1 = 1$ et $cd + c + d = 0$. Si la somme des nombres naturels est nulle, alors, en vertu du corollaire 2.8, chaque terme de la somme est nul. En particulier, $c = d = 0$; donc, $a = b = 1$. □

THÉORÈME 4.7. *Si un entier a divise l'unité, a est alors égal à* ± 1.

Démonstration. Posons que a divise l'unité, c'est-à-dire que $ab = 1$ pour un certain entier b. Alors $a^2b^2 = 1$. a^2 et b^2 étant des nombres naturels, selon le lemme 4.6 on a alors $a^2 = 1$. Par conséquent, selon le théorème 4.1, il vient

(1) $(-a)(-a) = 1.$

Puisque a ou $-a$ sont des nombres naturels, selon le lemme 4.6, il s'ensuit de $a^2 = 1$ et de l'égalité (1) que $a = 1$, ou $-a = 1$. □

THÉORÈME 4.8. *Si des entiers a et b sont associés (c'est-à-dire* $a \mid b$ *et* $b \mid a$*), alors* $a = \pm b$.

Démonstration. Par hypothèse, a divise b et b divise a, c'est-à-dire $b = ac$ et $a = bd$ pour des entiers c et d, donc,

(1) $a = acd.$

Si $a = 0$, alors $b = 0 \cdot c = 0$, et le théorème est vérifié. Si $a \neq 0$, il s'ensuit de (1) que $cd = 1$. Selon le théorème 4.7 de l'égalité $cd = 1$ on déduit que $d = \pm 1$. De plus, $a = bd$; donc, $a = \pm b$. □

Exercices

1. Soit $m\mathbf{Z} = \{mx \mid x \in \mathbf{Z}\}$, où m est un nombre naturel. Montrer que pour $m \neq 0$ il existe une application injective de l'ensemble $\mathbf{Z}$ sur $m\mathbf{Z}$.

2. Soit $\mathfrak{Z}' = \langle \mathbf{Z}, +, - \rangle$ un groupe additif des entiers. Montrer que l'ensemble $m\mathbf{Z}$, où m est un entier, est clos dans le groupe $\mathfrak{Z}$, c'est-à-dire est fermé relativement aux opérations $+$ et $-$.

3. Montrer qu'un ensemble non vide des entiers clos par rapport à l'addition n'est pas obligatoirement composé de multiples d'un entier fixé.

4. Montrer qu'un ensemble non vide des entiers clos dans le groupe $\mathfrak{Z}$ (fermé relativement aux opérations $+$ et $-$) est composé de multiples d'un certain entier fixé.

5. Etablir si, dans le groupe additif des entiers, sont des sous-groupes relativement aux opérations $+$, $-$ les ensembles des entiers suivants:

(a) l'ensemble de tous les nombres pairs;
(b) l'ensemble des nombres naturels;
(c) l'ensemble des nombres impairs.

6. Soient $\mathfrak{Z} = \langle \mathbf{Z}, +, - \rangle$ et m un entier fixé. Montrer que l'algèbre $m\mathfrak{Z} = \langle m\mathbf{Z}, +, - \rangle$ est un sous-groupe du groupe $\mathfrak{Z}$. Montrer que tout sous-groupe du groupe $\mathfrak{Z}$ coïncide avec le groupe $m\mathfrak{Z}$ pour un certain m naturel.

7. Démontrer qu'un groupe additif des entiers $\mathfrak{Z}$ est isomorphe au sous-groupe $m\mathfrak{Z}$ pour tout entier m autre que zéro.

8. Montrer que l'anneau $\mathfrak{Z}$ des entiers ne présente pas d'automorphismes différents de l'anneau identique.

9. Démontrer que l'anneau $\mathfrak{Z}$ des entiers ne présente pas de sous-anneaux différents de $\mathfrak{Z}$.

10. Soit $\mathcal{K}$ un anneau quelconque. Démontrer que dans l'anneau $\mathcal{K}$ il n'existe qu'un seul homomorphisme de l'anneau $\mathfrak{Z}$ des entiers.

11. Soit $\mathbf{Z}[\sqrt{2}] = \{m + n\sqrt{2} \mid m, n \in \mathbf{Z}\}$. Démontrer que l'algèbre $\mathfrak{Z}[\sqrt{2}] = \langle \mathbf{Z}[\sqrt{2}], +, -, \cdot, 1\rangle$ du type (2, 1, 2, 0), où $+, -, \cdot$ sont des opérations banales sur des nombres réels, est un anneau commutatif. Indiquer un automorphisme non trivial de cet anneau.

12. Démontrer qu'il n'existe pas d'homomorphismes de l'anneau $\mathfrak{Z}[\sqrt{2}]$ dans l'anneau $\mathfrak{Z}[\sqrt{3}]$ et que ces anneaux ne sont pas isomorphes.

13. Soit $K = \{\langle a, b\rangle \mid a, b \in \mathbf{Z}\}$, les opérations $+, -, \cdot, e$ sur l'ensemble K étant définies de la façon suivante:

$$\langle a, b\rangle + \langle c, d\rangle = \langle a + c, b + d\rangle;$$
$$-\langle a, b\rangle = \langle -a, -b\rangle;$$
$$\langle a, b\rangle \cdot \langle c, d\rangle = \langle ac, bd\rangle;$$
$$e = \langle 1, 1\rangle.$$

Montrer que l'algèbre $\langle K, +, -, \cdot, e\rangle$ est un anneau commutatif avec diviseurs de zéro.

14. Démontrer que pour tout n naturel:

(a) $5^{2n} - 1$ est divisible par 24;
(b) $4^n + 6n - 1$ est divisible par 9;
(c) $10^{3n} - 1$ est divisible par 3^3;
(d) $3^{2n} + 5$ n'est pas divisible par 8.

15. Démontrer que le produit de trois quelconques entiers consécutifs se divise par 6.

16. Démontrer que pour tout entier n:

(a) $n^3 - n$ est divisible par 3;
(b) $n^5 - n$ est divisible par 5;
(c) $n^7 - n$ est divisible par 7;
(d) $n(n^2 + 5)$ est divisible par 6;
(e) $n^5 - n$ est divisible par 30.

17. Montrer que si un entier n n'est pas divisible par 7, $n^3 - 1$ ou $n^3 + 1$ le sont.

18. Démontrer que pour tous entiers a et b:

(1) si $a \mid b$ et $b \neq 0$, alors $|a| \leqslant |b|$,
(2) si $a \mid b$ et $|b| < |a|$, alors $b = 0$.

19. Démontrer que pour tous entiers a et b

$$|ab| = |a| \cdot |b|, \qquad |a + b| \leqslant |a| + |b|.$$

20. Démontrer par récurrence sur n que pour tous entiers $a_1, \ldots, a_n$ on a l'inégalité $a_1^2 + \ldots + a_n^2 > 0$, excepté le cas où $a_1 = \ldots = a_n = 0$.

21. Démontrer que tout ensemble non vide des entiers limité inférieurement (supérieurement) présente un plus petit (un plus grand) élément.

22. Démontrer que pour tout entier a et tout entier positif b il existe un entier unique n tel que $nb \leqslant a < (n + 1)b$.

23. Démontrer la généralisation suivante du théorème de division avec reste: pour tous entiers a et b avec $b \neq 0$ il existe un couple unique d'entiers q, r pour lequel $a = bq + r$ et $0 \leqslant r < |b|$.

§ 5. Corps. Corps des nombres rationnels

Notion de corps. Donnons les principales définitions.

DÉFINITION. L'élément a de l'anneau $\mathcal{K}$ est nommé *élément inversible de l'anneau* s'il y a dans l'anneau un élément b tel que $ab = ba = 1_{\mathcal{K}}$. De plus, les éléments a et b sont dits *mutuellement inverses.*

DÉFINITION. On appelle *corps* un anneau commutatif dont le zéro est différent de l'unité, $0_{\mathcal{K}} \neq 1_{\mathcal{K}}$ et chaque élément non nul est un élément inversible de l'anneau.

DÉFINITION. Soit $\mathcal{F} = \langle F, +, -, \cdot, 1 \rangle$ un corps. Le groupe $\langle F, +, - \rangle$ est dit *groupe additif d'un corps.* Son élément neutre est appelé *zéro du corps* et est noté par le symbole 0 ou $0_{\mathcal{F}}$.

L'élément 1, élément neutre par rapport à la multiplication, est l'*unité du corps* et est également noté par le symbole $1_{\mathcal{F}}$.

DÉFINITION. On appelle *sous-corps du corps* $\mathcal{F}$ un sous-anneau du corps $\mathcal{F}$ dans lequel tout élément non nul est inversible. Le sous-corps du corps $\mathcal{F}$ différent de $\mathcal{F}$ est nommé *sous-corps propre.*

Il est clair que tout sous-corps est un corps.

DÉFINITION. Un corps est dit *simple* s'il ne possède pas de sous-corps propres.

Propriétés élémentaires du corps. Soient a, b des éléments du corps $\mathcal{F}$ et $b \neq 0$. L'équation $bx = a$ possède dans le corps la solution ab^{-1}; on vérifie sans peine que ab^{-1} est la solution unique de l'équation. L'élément ab^{-1} est noté par le symbole $\frac{a}{b}$ ou a/b.

THÉORÈME 5.1. *Soit $\mathcal{F} = \langle F, +, -, \cdot, 1 \rangle$ un corps. On a alors pour tous éléments a, b, c du corps:*

(1) *si $ab = 1$, alors $a \neq 0$ et $b = a^{-1}$;*

(2) *si $ac = bc$ et $c \neq 0$, alors $a = b$;*

(3) *si $ab = 0$, alors $a = 0$ ou $b = 0$;*

(4) *si $a \neq 0$ et $b \neq 0$, alors $ab \neq 0$;*

(5) $\frac{a}{b} = \frac{c}{d}$ *si et seulement si $ad = bc$, $b \neq 0$ et $d \neq 0$;*

(6) $$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd};$$

(7) $$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd};$$

(8) $$\frac{a}{b} + \frac{(-a)}{b} = 0 \quad \text{et} \quad -\left(\frac{a}{b}\right) = \frac{-a}{b};$$

(9) *si $a \neq 0$ et $b \neq 0$, alors* $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$;

(10) $$\frac{ac}{bc} = \frac{a}{b}.$$

Démonstration. (1) Si $ab = 1$, alors $a \neq 0$, car avec $a = 0$ $0 \cdot b = 1$ et $0 = 1$, ce qui n'est pas possible dans un corps. Puisque $a \neq 0$, il existe un élément a^{-1} inverse de a et $b = (a^{-1}a)b = a^{-1}(ab) - a^{-1} 1 = a^{-1}$.

(2) Si $ac = bc$ et $c \neq 0$, il existe un élément c^{-1} dans le corps et $a = (ac)c^{-1} = (bc)c^{-1} = b$, c'est-à-dire $a = b$.

(3) A partir de $ab = 0$ il s'ensuit que $a = 0$ ou $b = 0$. En effet, si $a \neq 0$, il existe un élément a^{-1} et $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$.

(4) Suivant la loi de contraposition de (3) il s'ensuit que

$\neg(a = 0 \vee b = 0) \to \neg(ab = 0)$, c'est-à-dire que $(a \neq 0 \wedge \wedge b \neq 0) \to (ab \neq 0)$.

(5) Soit $a/b = c/d$, c'est-à-dire $ab^{-1} = cd^{-1}$. On a alors $b \neq 0$, $d \neq 0$ et $ad = (ab^{-1})(bd) = cb^{-1} \cdot bd = cb$, c'est-à-dire $ad = cb$. Réciproquement : de l'égalité $ad = cb$ avec $b \neq 0$, $d \neq 0$ s'ensuivent les égalités $adb^{-1}d^{-1} = cbb^{-1}d^{-1}$ et $ab^{-1} = cd^{-1}$.

(6) Vu que $a/b = ab^{-1}$ et $c/d = cd^{-1}$, on a $\frac{a}{b} \pm \frac{c}{d} = ab^{-1} \pm cd^{-1} = add^{-1}b^{-1} \pm cbb^{-1}d^{-1} = (ad \pm bc)(bd)^{-1} = (ad \pm bc)/bd$.

(7) Pour $b \neq 0$ et $d \neq 0$

$$\frac{a}{b}\frac{c}{d} = ab^{-1}cd^{-1} = ac\,(bd)^{-1} = \frac{ac}{bd}.$$

(8) Pour $b \neq 0$

$$\frac{a}{b} + \frac{(-a)}{b} = ab^{-1} + (-a)\,b^{-1} = (a - a)\,b^{-1} = 0,$$

donc, $-(a/b) = -a/b$.

(9) Si $a \neq 0$ et $b \neq 0$, alors $(a/b)^{-1} = (ab^{-1})^{-1} = ba^{-1} = b/a$.

(10) Pour $b \neq 0$ et $c \neq 0$

$ac/bc = ac\,(bc)^{-1} = acc^{-1}b^{-1} = ab^{-1} = a/b$. □

Corps des nombres rationnels. Introduisons la notion de corps des fractions (des quotients) du domaine d'intégrité.

Définition. Posons que $\mathscr{F}$ est nommé *corps des fractions du domaine d'intégrité* $\mathscr{K}$ si sont satisfaites les conditions :

(α) $\mathscr{K}$ est un sous-anneau du corps $\mathscr{F}$;

(β) pour tout x de F il existe des éléments a, b de l'anneau $\mathscr{K}$ tels que $x = ab^{-1}$.

Théorème 5.2. *Pour tout domaine d'intégrité* $\mathscr{K}$ *on a un corps des fractions. Si* $\mathscr{F}$ *et* $\mathscr{P}$ *sont des corps des fractions de l'anneau* $\mathscr{K}$, *on a un isomorphisme du corps* $\mathscr{F}$ *sur le corps* $\mathscr{P}$ *faisant passer chaque élément de l'anneau* $\mathscr{K}$ *en lui-même.*

La démonstration de ce théorème est fournie au chapitre XIII (voir théorèmes 13.21 et 13.22).

L'anneau $\mathfrak{Z}$ des entiers est un domaine d'intégrité. Par conséquent, selon le théorème 5.2, il existe pour l'anneau $\mathfrak{Z}$ un corps des fractions et tous deux corps des fractions de l'anneau $\mathfrak{Z}$ sont isomorphes.

Définition. On appelle *corps des nombres rationnels* un corps des fractions d'un anneau des entiers. Les éléments du corps des nombres rationnels sont des *nombres rationnels*.

Il s'ensuit de la définition que tout nombre rationnel peut être représenté sous forme d'un quotient des deux entiers.

Notons que tout corps isomorphe à un corps des nombres rationnels est aussi un corps des nombres rationnels.

La relation d'ordre sur l'ensemble **Q** des nombres rationnels s'introduit au moyen de la relation d'ordre $<$ sur l'ensemble **Z** des entiers.

Définition. *La relation d'ordre* $<$ *sur l'ensemble* **Q** des nombres rationnels se définit de la façon suivante : pour deux nombres rationnels quelconques p/q et r/s, où $p, r \in \mathbf{Z}$ et $q, s \in \mathbf{N} \setminus \{0\}$, $\frac{p}{q} < \frac{r}{s}$ si et seulement si $ps < qr$.

Il est aisé de vérifier que $<$ sur l'ensemble **Q** des nombres rationnels est une relation d'ordre strict prolongeant la relation d'ordre sur l'ensemble **Z** des entiers.

Théorème 5.3. *La relation binaire* $<$ *sur l'ensemble* **Q** *des nombres rationnels est douée des propriétés suivantes* :

(1) *pour tous* a, b, c *de* **Q** *si* $a < b$ *et* $b < c$, *alors* $a < c$;

(2) *pour tous* a, b *de* **Q** *on n'a qu'une et rien qu'une des trois relations* $a < b$, $a = b$, $b < a$;

(3) *pour tous* a, b, c *de* **Q** *si* $a < b$, *alors* $a + c < b + c$;

(4) *pour tous* a, b, c *de* **Q** *si* $a < b$ *et* $0 < c$, *alors* $ac < bc$.

La démonstration du théorème est laissée au soin du lecteur.

Exercices

1. Etablir lesquels des ensembles suivants des nombres réels constituent des corps relativement aux opérations banales $+, -, \cdot$ sur ces ensembles :

(a) tous les nombres naturels ;
(b) tous les nombres rationnels à dénominateurs impairs ;
(c) tous les nombres de l'aspect $a + b\sqrt{2}$, a et b étant rationnels ;
(d) tous les nombres de l'aspect $a + b\sqrt{5}$, a et b étant rationnels ;
(e) tous les nombres de l'aspect $a + b\sqrt[3]{2}$, a et b étant rationnels ;
(f) tous les nombres de l'aspect $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, a, b et c étant rationnels.

2. Soit K un ensemble de toutes les matrices de la forme $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ à a et b rationnels. Démontrer que l'algèbre $\langle K, +, -, \cdot, e\rangle$, où $+, -, \cdot$ sont des opérations sur les matrices et $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, est un corps. Montrer que ce corps comporte un élément x tel que $x^2 = -e$.

3. Soit F un ensemble de toutes les matrices de la forme $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$ à a et b rationnels. Démontrer que l'algèbre $\mathcal{F} = \langle F, +, -, \cdot, e \rangle$, où $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, est un corps. Montrer que l'application $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \mapsto a + b\sqrt{2}$ est un isomorphisme du corps $\mathcal{F}$ sur le corps $\mathfrak{Q}(\sqrt{2})$.

4. Lesquels des anneaux $\mathfrak{Z}_2$, $\mathfrak{Z}_3$, $\mathfrak{Z}_4$, $\mathfrak{Z}_5$ et $\mathfrak{Z}_6$ sont des corps?

5. Démontrer qu'un corps est dépourvu de diviseurs de zéro.

6. Montrer que chaque sous-anneau d'un corps est un domaine d'intégrité.

7. Soit a un élément non nul d'un corps. Démontrer que pour tous entiers m et n les égalités $a^{m+n} = a^m a^n$ et $(a^m)^n = a^{mn}$ sont satisfaites.

8. Soient a, b et c des éléments quelconques du corps $\mathcal{F}$. Démontrer que de l'égalité $ab = ac$ s'ensuit $b = c$ si et seulement si $a \neq 0$.

9. Démontrer que l'intersection de toute collection de sous-corps du corps $\mathcal{F}$ est un sous-corps du corps $\mathcal{F}$.

10. Démontrer que tout domaine d'intégrité fini est un corps.

11. Montrer que le corps $\mathfrak{Q}$ des nombres rationnels ne présente pas de sous-corps différents de $\mathfrak{Q}$.

12. Démontrer que tout sous-corps du corps $\mathfrak{Q}(\sqrt{2})$ est soit $\mathfrak{Q}$, soit $\mathfrak{Q}(\sqrt{2})$.

13. Décrire tous les sous-anneaux du corps $\mathfrak{Q}$ des nombres rationnels.

14. Soit $\varphi: \mathcal{F} \to \mathcal{F}'$ un homomorphisme d'anneau du corps $\mathcal{F}$ dans le corps $\mathcal{F}'$. Montrer qu'avec l'application φ l'image du corps $\mathcal{F}$ est un sous-corps du corps $\mathcal{F}'$.

15. Démontrer qu'un homomorphisme d'anneau du corps $\mathcal{F}$ est soit une application zéro, soit un isomorphisme du corps $\mathcal{F}$ sur son image.

16. Soit $\varphi: \mathcal{F} \to \mathcal{F}'$ un homomorphisme d'anneau. Si $\mathcal{F}$ est un corps, $a, b \in F$ et $b \neq 0$, on a $\varphi(a/b) = \varphi(a)/\varphi(b)$; le démontrer.

17. Démontrer qu'une application identique est le seul automorphisme du corps $\mathfrak{Q}$ des nombres rationnels.

18. Montrer que tout corps composé de deux éléments est isomorphe au corps $\mathfrak{Z}_2$.

19. Démontrer qu'un anneau isomorphe au corps est lui-même un corps.

20. Montrer qu'il n'y a pas d'homomorphismes de l'anneau $\mathfrak{Z}_4$ dans le corps $\mathfrak{Z}_5$.

21. Démontrer que l'algèbre isomorphe au corps est elle-même un corps.

22. Montrer qu'un corps des fractions du corps $\mathcal{F}$ est isomorphe à $\mathcal{F}$.

23. Démontrer qu'un corps des fractions de l'anneau $\mathfrak{Z}[\sqrt{3}]$ est isomorphe au corps $\mathfrak{Q}(\sqrt{3})$.

24. Soient $\mathcal{K}$ et $\mathcal{K}'$ des domaines d'intégrité isomorphes. Démontrer que les corps des fractions de ces anneaux sont isomorphes.

§ 6. Système des nombres réels

Corps ordonnés. Le système algébrique $\langle F, < \rangle$ s'appelle *ensemble totalement ordonné* si sont remplies les conditions suivantes:

(α) pour tous a, b, c de F si $a < b$ et $b < c$, on a alors $a < c$;

(β) pour tout couple d'éléments a, b de F n'est satisfaite qu'une seule et rien qu'une seule des trois relations: $a < b$, $a = b$, $b < a$.

DÉFINITION. On appelle *corps ordonné* le système algébrique $\langle F, +, -, \cdot, 1, < \rangle$ qui est doué des propriétés:

(1) l'algèbre $\langle F, +, -, \cdot, 1\rangle$ est un corps;

(2) le système $\langle F, <\rangle$ est un ensemble totalement ordonné;

(3) pour tous a, b, c de F si $a < b$, alors $a + c < b + c$ (monotonie de l'addition);

(4) pour tous a, b, c de F si $a < b$ et $0 < c$, on a alors $ac < bc$ (monotonie de la multiplication).

L'élément a du corps ordonné est dit *positif* si $0 < a$. Par définition, $b > a$ si et seulement si $a < b$. Ensuite, par définition, $a \leqslant b$ si et seulement si $a < b$ ou $a = b$.

E x e m p l e. Soient $\langle Q, +, -, \cdot, 1\rangle$ un corps des nombres rationnels et $<$ la relation d'ordre banale sur l'ensemble Q. En vertu du théorème 5.3, les conditions (1)-(4) de la définition susmentionnée sont satisfaites. Par conséquent, le système $\langle Q, +, -, \cdot, 1\rangle$ est un corps ordonné. Ce système est dénommé *corps ordonné des nombres rationnels*.

THÉORÈME 6.1. *Soient* $\mathcal{F} = \langle F, +, -, \cdot, 1, <\rangle$ *un corps ordonné et* a, b, c, d *ses éléments quelconques. Il vient alors*

(1) $a < b$ *si et seulement si* $b - a > 0$;

(2) *pour tout* a *de* F *n'est satisfaite qu'une et rien qu'une des trois conditions*: $a < 0$, $a = 0$, $0 < a$;

(3) *si* $a > 0$ *et* $b > 0$, *alors* $a + b > 0$ *et* $ab > 0$, *autrement dit, l'ensemble d'éléments positifs d'un corps ordonné est fermé par rapport à l'addition et à la multiplication*;

(4) *si* $a < b$ *et* $c < d$, *on a alors* $a + c < b + d$;

(5) *si* $a < b$ *et* $c < 0$, *alors* $ac > bc$;

(6) *si* $a \neq 0$, *alors* $a^2 > 0$;

(7) $1 > 0$ *et* $n \cdot 1 > 0$ *pour tout* $n \neq 0$ *naturel*;

(8) *le corps* $\langle F, +, -, \cdot, 1\rangle$ *est un domaine d'intégrité.*

D é m o n s t r a t i o n. (1) En vertu de la monotonie de l'addition $a < b$ si et seulement si $a + (-a) < b + (-a)$. Donc, $a < b$ si et seulement si $b - a > 0$.

(2) L'affirmation (2) est vraie puisque $\langle F, <\rangle$ est un ensemble totalement ordonné (voir condition (β)).

(3) en raison de la monotonie de l'addition il s'ensuit de $a > 0$ et $b > 0$ que $a + b > b$ et $a + b > 0$. En vertu de la monotonie de la multiplication il s'ensuit de $a > 0$ et $b > 0$ que $ab > 0 \cdot b$ et $ab > 0$.

(4) En vertu de la monotonie de l'addition si $a < b$ et $c < d$, alors on a aussi $a + c < b + c$ et $b + c < b + d$. Donc, $a + c < b + d$.

(5) En vertu de (1) si $a < b$ et $c < 0$, on a $b - a > 0$ et $-c > 0$. En vertu de la monotonie de la multiplication on en déduit que $(b - a)(-c) > 0$ et $ac - bc > 0$. Donc, $ac > bc$.

(6) En vertu de la monotonie de la multiplication si $a > 0$, on a alors $a^2 > 0$. Si, par contre, $-a > 0$, alors $(-a)(-a) > 0$ et $a^2 > 0$.

(7) Dans le corps $1 \neq 0$. En vertu de (6) $1^2 = 1 > 0$. Comme l'ensemble des éléments positifs d'un corps ordonné est fermé par rapport à l'addition, il s'ensuit de $1 > 0$ que $n \cdot 1 > 0$ pour tout n naturel autre que zéro.

(8) En vertu du théorème 5.1 pour tous éléments a, b du corps si $a \neq 0$ et $b \neq 0$, on a $ab \neq 0$. Par conséquent, selon la loi de contraposition si $ab = 0$, alors $a = 0$ ou $b = 0$. Le corps $\langle F, +, -, \cdot, 1 \rangle$ est donc un domaine d'intégrité. □

DÉFINITION. La *valeur absolue de l'élément* a d'un corps ordonné est notée $|a|$ et est définie de la façon suivante:

$$|a| = \begin{cases} a & \text{si } a \geqslant 0, \\ -a & \text{si } (-a) > 0. \end{cases}$$

THÉORÈME 6.2. *Soient a et b des éléments quelconques d'un corps ordonné; on a alors*

(1) $|a| = |-a|$;
(2) $|a| \pm a \geqslant 0$;
(3) $|a + b| \leqslant |a| + |b|$;
(4) $|ab| = |a| \cdot |b|$;
(5) $|b| \leqslant a$ *si et seulement si* $-a \leqslant b \leqslant a$.

Démonstration. (1) L'égalité (1) se déduit directement de la définition de la valeur absolue de l'élément.

(2) Si $a \geqslant 0$, on a alors $|a| = a$, $|a| + a \geqslant 0$ et $|a| - a = 0$. Si, par contre, $(-a) > 0$, alors $|a| = -a$, $|a| - a = |a| + (-a) > 0$ et $|a| + a = 0$.

(3) Si $|a + b| = a + b$, en vertu de l'inégalité (2), on a

$$|a| + |b| - |a + b| = (|a| - a) + (|b| - b) \geqslant 0.$$

Si, par contre, $|a + b| = -(a + b)$, alors de même, en vertu de l'inégalité (2),

$$|a| + |b| - |a + b| = (|a| + a) + (|b| + b) \geqslant 0.$$

Donc, quel que soit le cas l'inégalité (3) est vraie.

(4) L'égalité (4) est vraie si a ou b est nul. Si les éléments a et b sont positifs, alors $|ab| = ab = |a| \cdot |b|$. Si $a < 0$ et $b < 0$, alors $ab = (-a)(-b) > 0$ et $|ab| = ab = (-a)(-b) = |a| \cdot |b|$. Si $a > 0$ et $b < 0$, alors $(-ab) > 0$ et $|ab| = -ab = a \cdot (-b) = |a| \cdot |b|$. Enfin, si $a < 0$ et $b > 0$, alors $(-ab) > 0$ et $|ab| = -ab = (-a)b = |a| \cdot |b|$.

(5) L'inégalité $|b| \leqslant a$ a lieu si et seulement si $(-b) \leqslant a$ et $b \leqslant a$. Donc, $|b| \leqslant a$ si et seulement si $-a \leqslant b$ et $b \leqslant a$, c'est-à-dire si $-a \leqslant b \leqslant a$. □

Système des nombres réels.

DÉFINITION. Un corps ordonné $\mathcal{F}$ présente un *ordre archimédien* si pour tous éléments positifs a et b il existe un nombre naturel n tel qu'on ait $na > b$.

Soit $\langle a_0, a_1, a_2, \ldots \rangle$ une suite infinie d'éléments du corps ordonné $\mathcal{F}$. On la note également $\langle a_k \rangle_{k \in N}$ ou $\langle a_k \rangle$.

DÉFINITION. L'élément a du corps ordonné $\mathcal{F}$ est nommé *limite de la suite* $\langle a_k \rangle$ *d'éléments du corps* si pour chaque élément positif ε du corps il y a un nombre naturel n_0 (dépendant de ε) tel que $| a_k - a | < \varepsilon$ pour tout $k \geqslant n_0$ naturel. La suite $\langle a_k \rangle$ possédant une limite dans le corps $\mathcal{F}$ est dite *convergente* dans ce corps.

DÉFINITION. La suite $\langle a_k \rangle$ d'éléments d'un corps ordonné $\mathcal{F}$ est dite *fondamentale* (de Cauchy) sur $\mathcal{F}$ si pour chaque élément positif ε du corps il existe un nombre naturel n_0 (dépendant de ε) tel qu'on ait $| a_k - a_n | < \varepsilon$ pour tous k et n naturels supérieurs à n_0.

DÉFINITION. Un corps ordonné est dit *complet* si toute suite de Cauchy d'éléments de ce corps converge dans ce dernier.

DÉFINITION. On appelle *système des nombres réels* un corps complet archimédien.

Soit $\langle \mathbf{R}, +, -, \cdot, 1, < \rangle$ un système des nombres réels. Dans ce cas l'algèbre $\langle \mathbf{R}, +, -, \cdot, 1 \rangle$ est un corps dit *corps des nombres réels*. L'ensemble $\mathbf{R}$ est nommé *ensemble des nombres réels*.

On peut démontrer que deux systèmes quelconques des nombres réels sont isomorphes. Donc, sont isomorphes tous deux corps des nombres réels.

THÉORÈME 6.3. *Pour deux nombres réels quelconques a et b avec $b > 0$ il y a un entier m et un nombre réel r tels que*

$$a = mb + r, \quad 0 \leqslant r < b.$$

Démonstration. 1°. Si $a = 0$, on a apparemment $m = r = 0$. Posons que $a > 0$. L'ensemble

$$M = \{n \in \mathbf{N} \mid (n + 1)\, b > a\}$$

des nombres naturels n'est pas vide, car le système des nombres réels est archimédien. L'ensemble des nombres naturels étant bien ordonné et M constituant un sous-ensemble non vide de l'ensemble $\mathbf{N}$, il existe dans M un plus petit élément. Soit m le plus petit élément de M, on a alors

$$mb \leqslant a < (m + 1)\, b, \quad 0 \leqslant a - mb < b.$$

En posant $a - mb = r$, il vient $a = mb + r$, $0 \leqslant r < b$.

2°. Posons que $a < 0$. Alors, selon la proposition démontrée au point 1°, il existe pour des nombres positifs $(-a)$ et b un nombre naturel k et un nombre réel s tels que

$$-a = kb + s, \quad 0 \leqslant s < b.$$

Par conséquent, $a = (-k)\, b + (-s)$. Si $s = 0$, on a la représentation cherchée. Si, par contre, $s > 0$, on a alors

$$a = (-k - 1) \cdot b + (b - s).$$

En posant $m = -k - 1$ et $r = b - s$, il vient

$$a = mb + r, \quad 0 \leqslant r < b. \ \square$$

Soit n un nombre naturel différent de zéro. Introduisons la notion de racine arithmétique de degré n d'un nombre réel positif. Mais au préalable démontrons le théorème suivant.

THÉORÈME 6.4. *Pour tout nombre positif a il existe un nombre réel positif unique c tel que $c^n = a$.*

D é m o n s t r a t i o n. Considérons la fonction $f = x^n - a$ définie sur un intervalle fermé $[0, b]$, où $b = a + 1$. La fonction f est continue sur cet intervalle et à ses extrémités acquiert des valeurs aux signes différents, vu que $f(0) < 0 < f(b)$. Appliquons le théorème des valeurs intermédiaires à la fonction f sur l'intervalle $[0, b]$. Il existe selon ce théorème un nombre réel $c \in [0, b]$ pour lequel $c^n - a = 0$, et, par suite,

(1) $\quad c^n = a.$

Apparemment, $c > 0$. Supposons que $d^n = a$ pour un nombre quelconque positif d. Si de plus $c < d$, alors $c^n < d^n = a$, ce qui est en contradiction avec (1). Mais si $c > d$, $c^n > d^n = a$, ce qui est aussi en contradiction avec (1). Donc, $d = c$. $\square$

DÉFINITION. Soient a un nombre réel positif et n un nombre naturel autre que zéro. Le nombre réel positif unique c pour lequel $c^n = a$ est nommé *racine arithmétique* ou *racine principale de degré n* de a et est noté par le symbole $c^{1/n}$ ou $\sqrt[n]{c}$.

Construction d'un système des nombres réels. On notera $\langle a_k \rangle_{k \in \mathbf{N}}$ ou $\langle a_k \rangle$ la suite $\langle a_0, a_1, a_2, \ldots \rangle$ des nombres rationnels. Définissons sur l'ensemble $\mathbf{Q}^{\mathbf{N}}$ de toutes les suites des nombres rationnels les opérations binaires $\oplus$, $\odot$, l'opération singulaire $\ominus$ et l'opération à aucune place $\bar{1}$:

$$\langle a_k \rangle \oplus \langle b_k \rangle = \langle a_k + b_k \rangle;$$

$$\ominus \langle a_k \rangle = \langle -a_k \rangle;$$

$$\langle a_k \rangle \odot \langle b_k \rangle = \langle a_k \cdot b_k \rangle;$$

$\bar{1} = \langle a_k \rangle$, où $a_k = 1$ pour tout k naturel.

Notons $F(\mathbf{Q})$ l'ensemble de toutes les suites de Cauchy sur le corps $\mathcal{Q}$ des nombres rationnels. Si $\langle a_k \rangle$ et $\langle b_k \rangle$ sont des éléments quelconques de l'ensemble $F(\mathbf{Q})$, les suites $\langle a_k \rangle \oplus \langle b_k \rangle$, $\ominus \langle a_k \rangle$, $\langle a_k \rangle \odot \langle b_k \rangle$ appartiennent également à l'ensemble $F(\mathbf{Q})$. Donc, l'ensemble $F(\mathbf{Q})$ est clos relativement aux opérations $\oplus$, $\ominus$, $\odot$.

Il est aisé de constater que l'algèbre $\langle F\,(Q), \oplus, \ominus, \odot, \bar{1}\rangle$ est un anneau commutatif.

Faisons opérer sur l'ensemble F (Q) la relation binaire $\equiv$: $\langle a_k\rangle \equiv \equiv \langle b_k\rangle$ si et seulement si la suite $\langle a_k - b_k\rangle$ converge vers zéro.

La relation $\equiv$ est réflexive, transitive et symétrique, c'est-à-dire est une relation d'équivalence sur l'ensemble F (Q). Convenons de désigner par le symbole $[\langle a_k\rangle]$ la classe d'équivalence à laquelle appartient la suite $\langle a_k\rangle$. L'ensemble de toutes les classes d'équivalence sera noté $\bar{F}$, $\bar{F} = F/\equiv$.

On montre sans peine que la relation $\equiv$ est une congruence dans l'anneau $\langle F\,(Q), \oplus, \ominus, \odot, 1\rangle$. Cela permet de définir sur l'ensemble $\bar{F}$ les opérations $+$, $-$, $\cdot$, 1 de la façon suivante:

$$[\langle a_k\rangle] + [\langle b_k\rangle] = [\langle a_k + b_k\rangle];$$

$$-[\langle a_k\rangle] = [\langle -a_k\rangle];$$

$$[\langle a_k\rangle]\cdot[\langle b_k\rangle] = [\langle a_k\cdot b_k\rangle];$$

$$1 - [\bar{1}].$$

L'algèbre $\langle \bar{F}, +, -, \cdot, 1\rangle$ est l'algèbre quotient de l'anneau $\langle F\,(Q), \oplus, \ominus, \odot, 1\rangle$ relativement à la congruence $\equiv$. On est en mesure de démontrer que l'algèbre $\langle \bar{F}, +, -, \cdot, 1\rangle$ est un corps.

Introduisons sur l'ensemble F (Q) la *relation d'ordre*: pour tous $\langle a_k\rangle$ et $\langle b_k\rangle$ de F (Q) on a

$$\langle a_k\rangle < \langle b_k\rangle,$$

s'il existe un nombre naturel n_0 et un nombre rationnel positif ε tels que $b_k - a_k \geqslant \varepsilon$ pour tout $k \geqslant n_0$.

La relation binaire $\equiv$ est une congruence par rapport à $<$, c'est-à-dire que pour tous $\langle a_k\rangle$, $\langle b_k\rangle$, $\langle c_k\rangle$ et $\langle d_k\rangle$ de F (Q), si

$$\langle a_k\rangle < \langle b_k\rangle, \quad \langle a_k\rangle \equiv \langle c_k\rangle \quad \text{et} \quad \langle b_k\rangle \equiv \langle d_k\rangle,$$

on a alors $\langle c_k\rangle < \langle d_k\rangle$.

Cela autorise d'introduire sur l'ensemble $\bar{F}$ la relation d'ordre: pour tous $[\langle a_k\rangle]$ et $[\langle b_k\rangle]$ de $\bar{F}$ on pose

$$[\langle a_k\rangle] < [\langle b_k\rangle] \quad \text{si} \quad \langle a_k\rangle < \langle b_k\rangle.$$

On est en mesure de démontrer que le système $\bar{\mathcal{F}} = \langle \bar{F}, +, -, \cdot, 1, <\rangle$ est un corps archimédien et toute suite de Cauchy sur le corps $\bar{\mathcal{F}}$ converge vers l'élément de ce corps. Le corps $\bar{\mathcal{F}}$ est donc un corps des nombres réels.

Exercices

1. Soient $\mathcal{F} = \langle F, +, -, \cdot, 1, < \rangle$ un corps ordonné et $a, b, c, d \in F$. Démontrer qu'alors:

(a) si $a + c < b + c$, on a $a < b$;
(b) si $a - b < a - c$, on a $b > c$;
(c) si $0 < c$ et $ac < bc$, on a $a < b$;
(d) $0 < \frac{1}{a} \leftrightarrow a > 0$;
(e) si $0 < a < b$, on a $0 < \frac{1}{b} < \frac{1}{a}$;
(f) si $a < b < 0$, on a $0 > \frac{1}{a} > \frac{1}{b}$;
(g) si au moins un des nombres a, b, c est différent de zéro, on a $a^2 + b^2 + c^2 > 0$.

2. Soient a, b des éléments du corps ordonné $\mathcal{F}$ et $a < b$. Démontrer qu'il existe dans $\mathcal{F}$ un élément c tel que $a < c < b$.

3. Démontrer que l'équation $x^2 = 2$ n'a pas de solutions dans un corps des nombres rationnels.

4. Démontrer que pour tout nombre réel positif a l'équation $x^2 = a$ possède une solution dans le corps des nombres réels.

5. Montrer que l'équation $x^2 + 1 = 0$ n'a pas de solutions dans un corps des nombres réels.

6. Soit $\mathbf{R}^+$ un ensemble de tous les nombres réels positifs. Démontrer que l'algèbre $\langle \mathbf{R}^+, \cdot, {}^{-1} \rangle$ est un groupe; il est nommé *groupe multiplicatif des nombres réels positifs*.

7. Soient a, b, c et d des nombres réels positifs. Démontrer que $a/b = c/d$ si et seulement si pour n'importe lesquels des entiers positifs m et n $na > mb \rightarrow nc > md$ et $na < mb \rightarrow nc < md$.

8. Démontrer qu'une application identique est l'unique isomorphisme d'un corps des nombres réels dans lui-même.

9. Démontrer qu'un système algébrique isomorphe au système des nombres réels est un système des nombres réels.

10. Soit $\mathbf{Q}^{\mathbf{N}}$ un ensemble de toutes les suites des nombres rationnels. Montrer que l'algèbre $\mathfrak{Q}^{\mathbf{N}} = \langle \mathfrak{Q}^{\mathbf{N}}, \oplus, \ominus, \odot, \bar{1} \rangle$, où

$\langle a_k \rangle \oplus \langle b_k \rangle = \langle a_k + b_k \rangle$;
$\ominus \langle a_k \rangle = \langle -a_k \rangle$;
$\langle a_k \rangle \odot \langle b_k \rangle = \langle a_k \cdot b_k \rangle$;
$\bar{1} = \langle a_k \rangle$, où $a_k = 1$ pour tout k naturel,

est un anneau commutatif.

11. Soit $F(\mathbf{Q})$ un ensemble de toutes les suites de Cauchy sur le corps $\mathfrak{Q} = \langle \mathbf{Q}, +, -, \cdot, 1 \rangle$. Montrer que $F(\mathbf{Q})$ est fermé dans l'anneau $\mathfrak{Q}^{\mathbf{N}}$ de toutes les suites des nombres rationnels et que l'algèbre $\mathcal{F}(\mathbf{Q}) = \langle F(\mathbf{Q}), \oplus, \ominus, \odot, \bar{1} \rangle$ est un anneau commutatif.

12. Supposons que $\langle a_k \rangle \equiv \langle b_k \rangle$ signifie que la suite $\langle a_k - b_k \rangle$ converge vers zéro. Démontrer que:

a) la relation $\equiv$ sur l'ensemble $F(\mathbf{Q})$ est une relation d'équivalence;
b) la relation $\equiv$ est une congruence dans l'anneau $\mathcal{F}(\mathbf{Q})$.

13. Montrer que si $\langle a_k\rangle \in F(\mathrm{Q})$, $a_k \neq 0$ pour tous les $k \in \mathrm{N}$ et la suite $\langle a_k\rangle$ ne converge pas vers zéro, on a alors

$$\langle 1/a_k\rangle \in F(\mathrm{Q}) \quad \text{et} \quad \langle a_k\rangle \odot \langle 1/a_k\rangle = \overline{1}.$$

14. Démontrer que l'algèbre quotient de l'anneau $\mathscr{F}$ (Q) par rapport à la congruence $\equiv$ est un corps.

15. Soit $\overline{F}$ l'ensemble quotient $F(\mathrm{Q})/\equiv$. Démontrer que le système $\langle \overline{F}, +, -, \cdot, 1, <\rangle$ est un corps archimédien.

16. Démontrer que dans le système $\langle \overline{F}, +, -, \cdot, 1, <\rangle$ toute suite de Cauchy des éléments de l'ensemble F converge vers l'élément de $\overline{F}$.

§ 7. Corps des nombres complexes

Extension complexe d'un corps. Soient $\mathscr{F} = \langle F, +, -, \cdot, 1\rangle$ un corps et t un élément (un symbole) n'appartenant pas au corps $\mathscr{F}$. L'expression de la forme $a + bt$, où a et b sont des éléments quelconques du corps $\mathscr{F}$, sera appelée *polynôme linéaire à t sur le corps* (ou la forme) $\mathscr{F}$. Les éléments a et b sont les *coefficients du polynôme* $a + bt$.

Deux polynômes linéaires à t sont dits *égaux* s'ils contiennent les mêmes termes (les mêmes coefficients) aux coefficients nuls près, qui peuvent être éliminés de l'expression (pour la forme). En particulier, pour tous éléments a et b du corps $\mathscr{F}$

(I) $a + 0\cdot t = a, \quad 0 + bt = bt.$

Désignons par K l'ensemble de tous les polynômes linéaires à t sur le corps $\mathscr{F}$:

$$K = \{a + bt \mid a, b \in F\}.$$

Sur l'ensemble K définissons les opérations $+$, $-$, $\cdot$ au moyen des formules suivantes:

(II) $(a + bt) + (c + dt) = (a + c) + (b + d)\,t;$

(III) $-(a + bt) = (-a) + (-b)\,t;$

(IV) $(a + bt)\cdot(c + dt) = (ac - bd) + (ad + bc)\,t.$

L'algèbre $\mathscr{K} = \langle K, +, -, \cdot, 1\rangle$, où 1 est l'unité du corps $\mathscr{F}$, sera appelée *algèbre des polynômes linéaires*.

THÉORÈME 7.1. *Soit $\mathscr{F} = \langle F, +, -, \cdot, 1\rangle$ un corps. L'algèbre $\mathscr{K} = \langle K, +, -, \cdot, 1\rangle$ des polynômes linéaires sur le corps $\mathscr{F}$ est un anneau commutatif et le corps $\mathscr{F}$ est son sous-anneau.*

D é m o n s t r a t i o n. Les opérations principales de l'algèbre $\mathscr{K}$ constituent des prolongements des opérations principales correspondantes du corps $\mathscr{F}$. En effet, en vertu des formules (I)-(IV) pour

10—01762

tous a et b de F

$$a + b = (a + 0 \cdot t) + (b + 0 \cdot t) = \\ = (a + b) + 0 \cdot t = a + b;$$

$$-a = -(a + 0 \cdot t) = (-a) + 0 \cdot t = -a;$$

$$a \cdot b = (a + 0 \cdot t) \cdot (b + 0 \cdot t) = a \cdot b + 0 \cdot t = a \cdot b.$$

En outre, l'élément 1 de l'algèbre $\mathcal{K}$ est l'unité du corps $\mathcal{F}$. Donc, le corps $\mathcal{F}$ est une sous-algèbre de l'algèbre $\mathcal{K}$:

(1) $\mathcal{F} \dashv \mathcal{K}$.

L'algèbre $\langle K, +, - \rangle$ est un groupe abélien. En effet, dans l'algèbre $\mathcal{K}$ (selon la formule (II)) l'addition est commutative et associative, vu que l'addition est commutative et associative dans le corps $\mathcal{F}$. Le zéro du corps $\mathcal{F}$ est un élément neutre par rapport à l'addition dans l'algèbre $\mathcal{K}$, puisque, en vertu des formules (I), (II), pour tout élément $a + bt$ de K

$$(a + b \cdot t) + 0 = (a + b \cdot t) + (0 + 0 \cdot t) = (a + bt).$$

Tout élément $a + b \cdot t$ de K possède son opposé, vu que $(a + b \cdot t) + ((-a) + (-b) \cdot t) = 0 + 0 \cdot t = 0$. On a ainsi établi que l'algèbre $\langle K, +, - \rangle$ est un groupe abélien.

L'algèbre $\langle K, \cdot, 1 \rangle$ est un monoïde commutatif. En effet, dans l'algèbre $\mathcal{K}$ (selon la formule (IV)) la multiplication est commutative en vertu de la commutativité de la multiplication dans le corps $\mathcal{F}$. Vérifions que dans l'algèbre $\mathcal{K}$ la multiplication est associative:

$$(a + b \cdot t) \cdot [(c + dt) \cdot (e + ft)] = (a + bt)\,[(ce - df) + (cf + de)\,t] = \\ = (ace - adf - bcf - bde) + \\ + (acf + ade + bce - bdf)\,t;$$

$$[(a + bt) \cdot (c + dt)] \cdot (e + ft) = [(ac - bd) + \\ + (ad + bc)\,t]\,(e + ft) = \\ = (ace - bde - adf - bcf) + \\ + (acf - bdf + ade + bce)\,t.$$

Donc,

$$(a + bt) \cdot [(c + dt) \cdot (e + ft)] = [(a + bt)\,(c + dt)]\,(e + ft).$$

L'unité du corps $\mathcal{F}$ est un élément neutre par rapport à la multiplication dans l'algèbre $\mathcal{K}$, car

$$(a + bt) \cdot 1 = (a + bt)\,(1 + 0 \cdot t) = a + bt.$$

On a ainsi établi que l'algèbre $\langle K, \cdot, 1 \rangle$ est un monoïde commutatif.

La multiplication dans l'algèbre $\mathscr{K}$ est distributive par rapport à l'addition. En effet,

$$[(a + bt) + (c + dt)]\cdot(e + ft) = [(a + c) + (b + d)\,t]\,(e + ft) = (ae + ce - bf - df) + (af + cf + be + de)t;$$

$$(a + bt)\cdot(e + ft) + (c + dt)\cdot(e + ft) = [(ae - bf) + (af + be)\,t] + [(ce - df) + (cf + de)\,t] = (ae - bf) + ce - df) + (af + be + cf + de)\,t.$$

Donc,

$$[(a + bt) + (c + dt)]\cdot(e + ft) = (a + bt)\cdot(e + ft) + (c + dt)\cdot(e + ft).$$

Bref, on a démontré que l'algèbre $\mathscr{K}$ est un anneau commutatif. En vertu de (1) le corps $\mathscr{F}$ est un sous-anneau de l'anneau $\mathscr{K}$. □

DÉFINITION. Soit $\mathscr{F} = \langle F, +, -, \cdot, 1\rangle$ un corps dans lequel le carré de chaque élément est différent de -1. Le corps $\mathscr{K}$ est appelé *extension complexe du corps* $\mathscr{F}$ si les conditions suivantes sont satisfaites :

(1) $\mathscr{F}$ est un sous-corps du corps $\mathscr{K}$;

(2) on a dans $\mathscr{K}$ un élément u tel que $u^2 = -1$;

(3) chaque élément z du corps $\mathscr{K}$ peut être représenté sous forme de $z = a + bu$, où $a, b \in F$.

PROPOSITION 7.2. *Soit $\mathscr{F}$ un corps dans lequel le carré de chaque élément est différent de -1. Soient $\mathscr{K}$ l'extension complexe du corps $\mathscr{F}$ et u un élément du corps $\mathscr{K}$ satisfaisant aux conditions* (2) *et* (3) *de la définition susmentionnée. Dans ce cas tout élément z du corps $\mathscr{K}$ peut être représenté de façon unique sous forme de $z = a + bu$, où $a, b \in F$.*

D é m o n s t r a t i o n. Soit z un élément quelconque du corps $\mathscr{K}$. Considérons deux représentations arbitraires de z sous la forme :

(4) $\quad z = a + bu, \quad z = c + du,$

où $a, b, c, d \in F$. Si $b \neq d$, alors $a + bu = c + du$ et $u = \frac{c-a}{b-d}$. Donc, $u = \frac{c-a}{b-d} \in F$ et $u^2 = -1$. Or, c'est contraire à la condition selon laquelle le carré de chaque élément du corps F est différent de -1. Donc, le cas où $b \neq d$ est impossible. Par conséquent, $b = d$ et en vertu de (4) $a = c$. □

THÉORÈME 7.3. *Soit $\mathscr{F} = \langle F, +, -, \cdot, 1\rangle$ un corps dans lequel le carré de tout élément est différent de -1. Il existe alors une extension complexe du corps $\mathscr{F}$.*

D é m o n s t r a t i o n. Soit K l'ensemble de tous les polynômes linéaires à t sur le corps $\mathscr{F}$:

(1) $\quad K = \{a + bt \mid a, b \in F\} \quad (t \notin F).$

La relation d'égalité et les opérations $+$, $-$, $\cdot$ se définissent sur l'ensemble K au moyen des formules (I)-(V). Selon le théorème 7.1 l'algèbre $\mathscr{K}$

$$\mathscr{K} = \langle K, +, - \cdot, 1\rangle$$

est un anneau commutatif et le corps $\mathscr{F}$ constitue un sous-anneau de l'anneau $\mathscr{K}$:

(2) $\mathscr{F} \dashv \mathscr{K}$.

Démontrons que l'anneau $\mathscr{K}$ est un corps. En vertu de (2) le zéro et l'unité du corps $\mathscr{F}$ sont le zéro et l'unité de l'anneau $\mathscr{K}$; donc $0_{\mathscr{K}} \neq 1_{\mathscr{K}}$. Il nous reste à montrer que pour tout élément non nul de K on a dans $\mathscr{K}$ un élément qui lui est opposé. Soit $a + bt \neq 0$, où $a, b \in F$. On a alors $a \neq 0$ ou $b \neq 0$. Par suite, $a^2 + b^2 \neq 0$, car dans le cas contraire $a^2 + b^2 = 0$ et $(a/b)^2 = -1$ (pour $b \neq 0$) ou $(b/a)^2 = -1$, ce qui est impossible vu l'hypothèse du théorème. En vertu des formules (II) et (V), il vient

$$(a+bt)\cdot\left(\frac{a}{a^2+b^2}+\frac{(-b)}{a^2+b^2}\,t\right)=1,$$

c'est-à-dire que l'élément $a + bt$ est inversible dans $\mathscr{K}$. L'anneau $\mathscr{K}$ est donc un corps.

L'élément t de K satisfait à la condition $t^2 = -1$. En effet, en vertu des formules (V) et (II), il vient

$$t\cdot t = (0 + 1\cdot t)\,(0 + 1\cdot t) = -1 + 0\cdot t = -1.$$

Enfin, en vertu de (2), le corps $\mathscr{F}$ est un sous-corps du corps $\mathscr{K}$. Par conséquent, le corps $\mathscr{K}$ est une extension complexe du corps $\mathscr{F}$. □

Théorème 7.4. *Soit* $\mathscr{F} = \langle F, +, -, \cdot, 1\rangle$ *un corps dans lequel le carré de tout élément est différent de* -1. *Soient* $\mathscr{K}$ *et* $\mathscr{K}'$ *des extensions complexes du corps* $\mathscr{F}$. *Il existe alors un isomorphisme du corps* $\mathscr{K}$ *sur le corps* $\mathscr{K}'$ *qui laisse invariants tous les éléments du corps* $\mathscr{F}$.

D é m o n s t r a t i o n. Il existe dans $\mathscr{K}$ un élément u tel que $u^2 = -1$ et tout élément du corps $\mathscr{K}$ se représente de façon unique sous forme de $a + bu$, où $a, b \in F$. De façon analogue, il existe dans $\mathscr{K}'$ un élément t tel que $t^2 = -1$ et chaque élément du corps $\mathscr{K}'$ se représente de façon unique sous forme de $a + bt$, où $a, b \in F$. Notons ψ l'application (qui est injective) de K sur K' associant à l'élément $a + bu$ de K l'élément $a + bt$ de K'. En outre, ψ respecte les opérations principales du corps $\mathscr{K}$. En effet, puisque

$$(a + bu) + (c + du) = (a + c) + (b + d)\,u,$$

$$-(a + bu) = (-a) + (-b)\,u,$$

$$(a + bu)\,(c + du) = (ac - bd) + (ad + bc)\,u,$$

on a

$$\psi((a+bu)+(c+du)) = (a+c)+(b+d)t = (a+bt) + \\ + (c+dt) = \psi(a+bu)+\psi(c+du),$$

$$\psi(-(a+bu)) = (-a)+(-b)t = -(a+bt) = \\ = -\psi(a+bu),$$

$$\psi((a+bu)(c+du)) = (ac-bd)+(ad+bc)t = \\ = (a+bt)\cdot(c+dt) = \psi(a+bu)\cdot\psi(c+du).$$

De plus, $\psi(1) = 1$ et $\psi(a) = a$ pour tout élément a du corps $\mathscr{F}$. Ainsi ψ est une application isomorphe du corps $\mathscr{K}$ sur le corps $\mathscr{K}'$ qui laisse invariants tous les éléments du corps $\mathscr{F}$. □

Corps des nombres complexes. Dans un corps ordonné le carré de tout élément non nul est positif. Donc, dans un corps des nombres réels le carré de tout nombre réel est différent de -1. En vertu du théorème 7.3 il existe une extension complexe du corps des nombres réels $\mathscr{R}$. Selon le théorème 7.4 toutes deux extensions complexes du corps $\mathscr{R}$ des nombres réels sont isomorphes.

Définition. On appelle *corps des nombres complexes* une extension complexe du corps des nombres réels.

Soit $\mathscr{R} = \langle \mathbf{R}, +, -, \cdot, 1\rangle$ un corps des nombres réels. Soit $\mathscr{C}$ un corps des nombres complexes, extension complexe du corps $\mathscr{R}$. L'ensemble de base du corps $\mathscr{C}$ est noté $\mathbf{C}$. Les éléments de l'ensemble $\mathbf{C}$ sont nommés *nombres complexes*. Désignons par i un nombre complexe pour lequel $i^2 = -1$, de sorte que tout nombre complexe z de $\mathbf{C}$ peut être représenté sous forme de $z = a + bi$, où $a, b \in \mathbf{R}$. Cette représentation est nommée *forme algébrique du nombre z*. Le nombre i est dit *unité imaginaire du corps des nombres complexes.*

Théorème 7.5. *Soient $\mathscr{C} = \langle \mathbf{C}, +, -, \cdot, 1\rangle$ un corps des nombres complexes, extension complexe du corps $\mathscr{R}$ des nombres réels et a, b, c, d des nombres réels arbitraires. On a alors*

(1) $a + bi = c + di$ *si et seulement si* $a = c$ *et* $b = d$;

(2) $(a + bi) + (c + di) = (a + c) + (b + d)\,i$;

(3) $-(a + bi) = (-a) + (-b)\,i$;

(4) $(a + bi)(c + di) = (ac - bd) + (ad + bc)\,i$;

(5) *si* $a + bi \neq 0$, *alors* $(a+bi)^{-1} = \frac{a}{a^2+b^2} + \frac{(-b)}{a^2+b^2}\cdot i$.

Démonstration. Soit $a+bi=c+di$. Si $b=d$, on a $a=c$. Mais si $b\neq d$ il s'ensuit que $i=\frac{c-a}{b-d}\in\mathbf{R}$ et $\left(\frac{c-a}{b-d}\right)^2=-1$, ce qui est impossible. Donc, le cas de $b\neq d$ est inacceptable. $\mathscr{C}$ étant un corps, on a les égalités (2), (3) et (4).

Soit $a + bi \neq 0$. En vertu de (1) $a \neq 0$ ou $b \neq 0$ et $a - bi \neq 0$. Etant donné que le produit de deux éléments quelconques non nuls du corps $\mathscr{C}$ est différent de zéro, on a $(a + bi)(a - bi) = a^2 + b^2 \neq$ $\neq 0$. Par conséquent,

$$(a+bi)^{-1} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} + \frac{(-b)}{a^2+b^2}\, i. \ \square$$

DEFINITION. On appelle *corps numérique* tout sous-corps d'un corps des nombres complexes.

Tout corps numérique comporte un sous-corps des nombres rationnels. En effet, soit $\mathscr{F} = \langle F, +, -, \cdot, 1\rangle$ un corps numérique quelconque. Vu que $0, 1 \in F$ et l'ensemble F est clos relativement aux opérations $+, -$, on en déduit que $n = 1 + \ldots + 1 \in F$ et $-n \in F$. Donc, F contient tous les nombres entiers. L'ensemble F est fermé par rapport à la division et, par suite, renferme tous les éléments de la forme mn^{-1} notés m/n. Donc, F renferme l'ensemble Q de tous les nombres rationnels. L'ensemble Q est clos relativement aux opérations principales du corps $\mathscr{F}$ et tout élément non nul de Q est inversible dans Q. Il s'ensuit que l'algèbre $\mathscr{Q}$, $\mathscr{Q} = \langle Q, +, -, \cdot, 1\rangle$, est un sous-corps du corps $\mathscr{F}$. Par conséquent, le corps numérique $\mathscr{F}$ contient un sous-corps $\mathscr{Q}$ des nombres rationnels.

DEFINITION. On appelle *anneau numérique* tout sous-anneau d'un corps des nombres complexes.

Ainsi, par exemple, les anneaux $\mathfrak{Z}$, $\mathscr{Q}$, $\mathscr{C}$ sont numériques. Le sous-anneau du corps $\mathscr{C}$ engendré par l'élément i et noté $\mathfrak{Z}[i]$ est un corps numérique.

Nombres conjugués. Si $z = a + bi$, où $a, b \in \mathbf{R}$, alors le nombre $a - bi$ est noté $\bar{z}$.

DEFINITION. Les nombres complexes $z = a + bi$ et $\bar{z} = a - bi$ sont dits *conjugués*.

Rappelons que l'application isomorphe d'un corps sur lui-même est appelée automorphisme du corps.

THEOREME 7.6. *Si z et z' sont des nombres complexes quelconques, on a alors*

(1) $\overline{z + z'} = \bar{z} + \bar{z}'$;

(2) $\overline{(-z)} = -\bar{z}$;

(3) $\overline{z \cdot z'} = \bar{z} \cdot \bar{z}'$;

(4) $\overline{(\bar{z})} = z$;

(5) $z = \bar{z}$ *si et seulement si* $z \in \mathbf{R}$;

(6) *si* $z = a + bi$, *alors* $z \cdot \bar{z} = a^2 + b^2$.

La démonstration du théorème est laissée au soin du lecteur.

COROLLAIRE 7.7. *L'application d'un corps des nombres complexes $\mathscr{C}$ en lui-même qui fait correspondre à tout nombre complexe z son conjugué*

$\bar{z}$ est un automorphisme du corps $\mathscr{C}$ qui laisse invariants les nombres réels.

Module d'un nombre complexe. Introduisons la notion de module d'un nombre complexe.

DÉFINITION. On appelle *module d'un nombre complexe* $a + bi$ $(a, b \in \mathbf{R})$ la racine carrée arithmétique du nombre $a^2 + b^2$, c'est-à-dire le nombre $(a^2 + b^2)^{1/2}$. Le module d'un nombre complexe $z = a + bi$ est noté $|z|$ ou $|a + bi|$. Ainsi, par définition, $|z|^2 = a^2 + b^2$.

THÉORÈME 7.8. *Pour tous nombres complexes z et u, on a*

(1) $|z|^2 = z \cdot \bar{z}$;

(2) $|z| = 0$ *si et seulement si* $z = 0$;

(3) $|zu| = |z| \cdot |u|$;

(4) $|z^{-1}| = |z|^{-1}$ *pour* $z \neq 0$;

(5) $|z + u| \leqslant |z| + |u|$;

(6) $|z| - |u| \leqslant |z + u|$;

(7) $||z| - |u|| \leqslant |z + u|$.

Démonstration. (1) Si $z = a + bi$, $\bar{z} = a - bi$ et $z \cdot \bar{z} = a^2 + b^2 = |z|^2$.

(2) Si $|z| = |a + bi| = 0$, alors $|z|^2 = a^2 + b^2 = 0$. Mais comme a et b sont des nombres réels, il s'ensuit de $a^2 + b^2 = 0$ que $a = b = 0$, c'est-à-dire que $z = 0$.

(3) En vertu de (1)

$$|zu|^2 = (zu)\,\overline{(zu)} = (zu)\,(\bar{z}\bar{u}) = (z\bar{z})\,(u\bar{u}) = |z|^2\,|u|^2 = (|z| \cdot |u|)^2.$$

De l'égalité $|zu|^2 = (|z| \cdot |u|)^2$ on déduit la formule (3).

(4) Selon (3), pour $z \neq 0$

$$|z \cdot z^{-1}| = |z| \cdot |z^{-1}| = 1.$$

Par suite, $|z^{-1}| = |z|^{-1}$.

(5) De (1) il vient

$$|z + 1|^2 = (z + 1) \cdot \overline{(z + 1)} = |z|^2 + z + \bar{z} + 1.$$

De plus, si $z = a + bi$, $z + \bar{z} = 2a \leqslant 2\,(a^2 + b^2)^{1/2} = 2\,|z|$. Aussi $|z + 1|^2 \leqslant (|z| + 1)^2$; par conséquent, $|z + 1| \leqslant |z| + 1$. En s'appuyant sur la formule (3) et sur la dernière inégalité, on conclut que pour $u \neq 0$

$$|z + u| = |u\,(zu^{-1} + 1)| = |u|\,|zu^{-1} + 1| \leqslant \leqslant |u|\,(|zu^{-1}| + 1) = |u|\,(|z|\,|u|^{-1} + 1).$$

Donc, $|z + u| \leqslant |z| + |u|$.

(6) Vu que $z = -u + (z + u)$ et $| -u | = | u |$, en vertu de (5) $| z | \leqslant | -u | + | z + u | = | u | + | z + u |$. Donc, $| z | - | u | \leqslant | z + u |$.

(7) Puisque le nombre $| \, | z | - | u | \, |$ est égal à $| z | - | u |$ ou $| u | - | z |$, l'inégalité (7) se déduit de l'inégalité (6). □

Interprétation géométrique des nombres complexes. A chaque nombre complexe $z = a + bi$ faisons correspondre un point $M(a, b)$ du plan (à système des coordonnées rectangulaire) d'abscisse a et d'ordonnée b. Le point $M(a, b)$ est dit *affixe de* $a + bi$.

Pour tous deux nombres complexes $a + bi$ et $c + di$ l'égalité $a + bi = c + di$ n'a lieu que si et seulement si $a = c$ et $b = d$. Aussi l'application associant à chaque nombre complexe $a + bi$ le point $M(a, b)$ du plan des coordonnées constitue-t-elle une application injective de l'ensemble **C** des nombres complexes sur l'ensemble des points du plan des coordonnées. Le plan des coordonnées dont les points sont la représentation géométrique des nombres complexes est appelé *plan complexe*.

Soient r et φ les coordonnées polaires du point M (O est l'origine, Ox l'axe polaire). Alors $r = (a^2 + b^2)^{1/2}$, autrement dit, r est le module du nombre complexe $a + bi$.

Les nombres réels sont représentés par des points de l'axe des abscisses; c'est justement pourquoi on appelle *axe réel* l'axe des abscisses. Les points de l'axe des ordonnées représentent des *nombres purement imaginaires*, c'est-à-dire des nombres de la forme bi, où $b \in \mathbf{R}$, aussi l'axe des ordonnées est-il nommé *axe imaginaire*.

Les *nombres conjugués* z et $\bar{z}$ sont figurés par des points symétriques par rapport à l'axe réel. Les *nombres* z et $-z$ *mutuellement opposés* sont représentés par des points symétriques par rapport à l'origine des coordonnées.

Les affixes des nombres complexes de même module r, $r > 0$, se disposent sur un cercle de rayon r et ayant pour centre l'origine des coordonnées.

Représentons sur un plan complexe les nombres complexes $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i$ ainsi que leur somme $z_3 = (a_1 + a_2) + (b_1 + b_2) i$ par les points M_1, M_2 et M_3 respectivement. Le segment géométriquement orienté OM_3 s'obtient à partir des segments orientés OM_1 et OM_2 suivant la règle du parallélogramme.

Exercices

1. Chercher sur le plan les affixes des nombres complexes 1, i, $1 + i$, $1 - i$, $-1 - i$, $1 + i\sqrt{3}$, $\sqrt{3} - i$.

2. Soient donnés un nombre réel positif a et un nombre complexe c. Chercher l'ensemble des points du plan constituant les affixes des nombres complexes z et qui satisfont aux conditions:

(a) $| z | = a$; (b) $| z - c | = a$;

(c) $| z | < a$; (d) $| z - c | < a$;

(e) $|z-1| \leqslant 1$; (f) $|z-1-i| < \sqrt{2}$;

(g) $|z-1|+|z+1| = 2$.

3. Résoudre les équations:

(a) $(1-i)\bar{z} - 3iz = 2-i$;

(b) $z\cdot\bar{z} - 2\bar{z} = 3-i$;

(c) $z\cdot\bar{z} + 3(z-\bar{z}) = 4+3i$;

(d) $z\cdot\bar{z} + 3(z+\bar{z}) = 7$;

(e) $z\cdot\bar{z} + 3(z+\bar{z}) = 3i$.

4. Montrer que pour tous nombres complexes z_1 et z_2 on a l'égalité $|z_1+z_2|^2 + |z_1-z_2|^2 = 2(|z_1|^2 + |z_2|^2)$. Quelle est l'interprétation géométrique de cette égalité?

5. Résoudre le système d'équations:

(a) $ix + (1+i)y = 3-i$; $(1-i)x - (6-i)y = 4$;

(b) $(2+i)x - (3+i)y = i$; $(3-i)\bar{x} + (2+i)\bar{y} = -i$.

6. Résoudre les équations (dans un corps des nombres complexes):

(a) $z^2 - (4+3i)z + 1 + 5i = 0$;

(b) $z^2 + 5z + 9 = 0$;

(c) $z^2 + z + 1 + i = 0$;

(d) $z^3 + 1 = 0$;

(e) $z^4 + 1 = 0$.

7. Démontrer que dans un corps des nombres complexes il n'existe qu'un seul automorphisme différent de l'automorphisme identique qui transforme de nouveau les nombres réels en des nombres réels.

8. Démontrer que chaque anneau numérique contient un sous-anneau des entiers.

9. Soit C_1 un ensemble de toutes les matrices carrées d'ordre deux de l'aspect $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ à a et b réels. Démontrer que l'algèbre $\langle C_1, +, -, \cdot, e\rangle$ du type (2, 1, 2, 0), où $+$, $-$, $\cdot$ sont des opérations banales sur les matrices et $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ est un corps isomorphe au corps des nombres complexes.

10. Soit K un ensemble des nombres complexes de la forme $m + ni$ à m et n entiers. Montrer que l'algèbre $\langle K, +, -, \cdot, 1\rangle$ est un domaine d'intégrité (un anneau d'intégrité). Cet anneau est nommé *anneau des entiers de Gauss.*

11. Décrire un sous-corps d'un corps des nombres complexes engendré par le nombre i et des nombres rationnels.

§ 8. Forme trigonométrique d'un nombre complexe. Extraction des racines à partir des nombres complexes

Forme trigonométrique d'un nombre complexe. A côté de la forme algébrique du nombre complexe on utilise fréquemment la forme trigonométrique.

PROPOSITION 8.1. *Pour tous nombres réels x et y satisfaisant à la condition*

1) $x^2 + y^2 = 1$,

il existe un nombre réel unique φ, *tel que*

(2) $x = \cos\varphi, \quad y = \sin\varphi, \quad 0 \leqslant \varphi < 2\pi.$

D é m o n s t r a t i o n. Supposons que les nombres réels x et y satisfont à la condition (1), alors on a

(3) $|x| \leqslant 1.$

Tout nombre réel satisfaisant à la condition (3) appartient au domaine des valeurs de la fonction cos de l'intervalle fermé $[0, \pi]$. Il existe donc un nombre réel ψ tel que

(4) $x = \cos\psi, \quad 0 \leqslant \psi \leqslant \pi.$

En vertu de (1) et (4) $y^2 = \sin^2\psi$ et $y = \pm\sin\psi$. Si $y = \sin\psi$, posons $\varphi = \psi$. Mais si $y = -\sin\psi$, posons $\varphi = 2\pi - \psi$. En tout cas le nombre réel φ satisfait aux conditions (2).

Supposons que θ est un nombre réel quelconque satisfaisant aux conditions

(5) $x = \cos\theta, \quad y = \sin\theta, \quad 0 \leqslant \theta < 2\pi.$

Admettons que $\theta \leqslant \varphi$, alors

$$\sin(\varphi - \theta) = \sin\varphi\cos\theta - \cos\varphi\sin\theta = yx - xy = 0.$$

Or $0 \leqslant \varphi - \theta < 2\pi$, aussi l'égalité $\sin(\varphi - \theta) = 0$ n'a-t-elle lieu que pour $\varphi - \theta = 0$ ou $\varphi - \theta = \pi$. Si $\varphi - \theta = \pi$, $\cos\varphi = -\cos\theta = -x = -\cos\varphi$, $\sin\varphi = -\sin\theta = -y = -\sin\varphi$; à partir des égalités $\cos\varphi = -\cos\varphi$, $\sin\varphi = -\sin\varphi$ il s'ensuit que $\cos\varphi = \sin\varphi = 0$, ce qui est impossible. Donc, le cas où $\varphi - \theta = \pi$ est impossible. Par conséquent, $\varphi - \theta = 0$ et $\varphi = \theta$. □

THÉORÈME 8.2. *Pour tout nombre complexe* z *autre que zéro il y a un couple unique des nombres réels* r *et* φ *tel que*

(1) $z = r(\cos\varphi + i\sin\varphi), \quad 0 < r, \quad 0 \leqslant \varphi < 2\pi.$

D é m o n s t r a t i o n. Si r satisfait aux conditions (1), on a alors $|z|^2 = r^2(\cos^2\varphi + \sin^2\varphi) = r^2$ et $r = |z|$. Il n'existe donc pas plus d'un nombre réel r satisfaisant aux conditions (1).

Soit $z = a + bi \neq 0$, où a, b sont des nombres réels. Posons $r = (a^2 + b^2)^{1/2}$, $r > 0$. Alors $(a/r)^2 + (b/r)^2 = 1$. En vertu de la proposition 8.1 il existe un nombre réel unique φ satisfaisant aux conditions

(2) $a/r = \cos\varphi, \quad b/r = \sin\varphi, \quad 0 \leqslant \varphi < 2\pi.$

Comme $r > 0$ et $z = r\left(\frac{a}{r} + \frac{b}{r}i\right)$, il s'ensuit de (2)

(3) $z = r(\cos\varphi + i\sin\varphi), \quad 0 \leqslant \varphi < 2\pi.$

D'un autre côté, de (3) se déduisent les égalités $a + bi = r \cos \varphi + r \sin \varphi \cdot i$, $a = r \cos \varphi$, $b = r \sin \varphi$. Donc, les conditions (2) découlent des conditions (3). Par suite, les conditions (2) et (3) sont équipotentes pour $r > 0$. Il n'existe donc qu'un couple unique des nombres réels satisfaisant aux conditions (1). □

DÉFINITION. On appelle *forme trigonométrique du nombre complexe* z sa représentation $z = r (\cos \varphi + i \sin \varphi)$, où r et φ sont des nombres réels et $r \geqslant 0$.

THÉORÈME 8.3. *Soient*

(1) $z = r (\cos \varphi + i \sin \varphi), \quad r > 0,$

(2) $z = r_1 (\cos \psi + i \sin \psi), \quad r_1 > 0,$

deux représentations du nombre complexe z sous forme trigonométrique. On a alors $r = r_1 = |z|$ et il y a un entier k tel que $\varphi - \psi = 2\pi k$.

Démonstration. On a établi dans le théorème 8.2 que de (1) et (2) s'ensuivent respectivement les égalités $r = |z|$ et $r_1 = |z|$ ou $r = r_1 = |z|$. Selon le théorème 6.3 il existe pour le couple de nombres φ et 2π un nombre réel α et un entier m tels que

(3) $\varphi = 2\pi m + \alpha, \quad 0 \leqslant \alpha < 2\pi.$

De façon analogue, pour les nombres ψ et 2π il existe un nombre réel β et un entier n tels que

(4) $\psi = 2\pi n + \beta, \quad 0 \leqslant \beta < 2\pi.$

Sur la base des formules (1), (3), il vient $r = |z|$ et

(5) $z = |z| (\cos \alpha + i \sin \alpha).$

En vertu des formules (2), (4), on aboutit à $r_1 = |z|$ et à

(6) $z = |z| (\cos \beta + i \sin \beta).$

Puisque $|z| \neq 0$, à partir de (5) et (6) on tire

(7) $\cos \alpha + i \sin \alpha = \cos \beta + i \sin \beta.$

Comme $0 \leqslant \alpha, \beta < 2\pi$, selon le théorème 8.2, on obtient de (7)

(8) $\alpha = \beta.$

Sur la base de (3), (4) et (8) on conclut que $\varphi - \psi = 2\pi k$, où $k = m - n$. □

THÉORÈME 8.4. *Soient* $z = |z| (\cos \varphi + i \sin \varphi)$, $z_1 = |z_1| \times (\cos \psi + i \sin \psi)$, *où φ et ψ sont des nombres réels, alors*

(1) $zz_1 = |z| \, |z_1| \, [\cos (\varphi + \psi) + i \sin (\varphi + \psi)]$;

(2) $\frac{z}{z_1} = \frac{|z|}{|z_1|} [\cos (\varphi - \psi) + i \sin (\varphi - \psi)]$ *pour* $z_1 \neq 0$;

(3) $z^n = |z|^n (\cos n\varphi + i \sin n\varphi)$ *pour tout n naturel*;

(4) $(\cos \varphi + i \sin \varphi)^n = \cos n\varphi + i \sin n\varphi.$

D é m o n s t r a t i o n. En vertu de la distributivité de la multiplication des nombres complexes par rapport à l'addition, il vient

$$z \cdot z_1 = |z| \cdot |z_1| \,[(\cos\varphi\cos\psi - \sin\varphi\sin\psi) + (\cos\varphi\sin\psi + \cos\psi\sin\varphi)\, i].$$

D'où s'ensuit la formule (1), puisque

$$\cos\varphi\cos\psi - \sin\varphi\sin\psi = \cos(\varphi+\psi);$$
$$\cos\varphi\sin\psi + \cos\psi\sin\varphi = \sin(\varphi+\psi).$$

En vertu de la formule (1), on obtient

$$(\cos\psi + i\sin\psi)(\cos(-\psi) + i\sin(-\psi)) = \cos 0 + i\sin 0 = 1,$$

et, par suite,

$$\frac{1}{\cos\psi + i\sin\psi} = \cos(-\psi) + i\sin(-\psi),$$

et pour $z_1 \neq 0$

$$\frac{1}{z_1} = \frac{1}{|z_1|}(\cos(-\psi) + i\sin(-\psi)).$$

Par conséquent, selon la formule (1)

$$\frac{z}{z_1} = z\cdot\frac{1}{z_1} = \frac{|z|}{|z_1|}\cdot[\cos(\varphi-\psi) + i\sin(\varphi-\psi)].$$

La formule (3) se démontre par récurrence sur n en s'inspirant de la formule (1). La formule (4) s'obtient à partir de la formule (3) pour $|z| = 1$. □

Les formules (3) et (4) sont nommées *formules de Moivre*.

Racines n-ièmes de l'unité. Soit n tout nombre naturel différent de zéro.

DÉFINITION. Un nombre complexe w satisfaisant à la condition $w^n = 1$ est nommé *racine n-ième de l'unité*.

THÉORÈME 8.5. *Il existe exactement n différentes racines n-ièmes de l'unité qui s'obtiennent toutes par la formule*

$$w_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} \quad \textit{avec } k = 0, 1, \ldots, n-1.$$

D é m o n s t r a t i o n. Chacun des nombres w_k constitue une racine n-ième de l'unité, car, selon la formule de Moivre,

$$w_k^n = \left(\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}\right)^n = \cos 2\pi k + i\sin 2\pi k = 1.$$

Les nombres réels $\frac{2\pi\cdot 0}{n}, \frac{2\pi\cdot 1}{n}, \ldots, \frac{2\pi(n-1)}{n}$ sont non négatifs, inférieurs au nombre 2π et diffèrent deux par deux. Donc, selon le

théorème 8.2, les nombres complexes $w_0, w_1, \ldots, w_{n-1}$ diffèrent deux par deux.

Il nous reste à montrer qu'une racine n-ième quelconque de l'unité appartient à l'ensemble $\{w_0, w_1, \ldots, w_{n-1}\}$. Selon le théorème 8.2 le nombre w peut être figuré sous la forme $w = |w| (\cos\varphi + i \sin\varphi)$, le nombre réel φ satisfaisant aux conditions

(1) $0 \leqslant \varphi < 2\pi$.

Comme $w^n = 1$, $|w|^n = 1$ et, selon le théorème 6.4, $|w| = 1$. Par conséquent, $w = \cos\varphi + i \sin\varphi$. Selon la formule de Moivre $w^n = \cos n\varphi + i \sin n\varphi$. Aussi l'égalité $w^n = 1$ peut-elle être écrite sous la forme

(2) $\cos n\varphi + i \sin n\varphi = \cos 0 + i \sin 0$.

Selon le théorème 8.3, il s'ensuit de (2) que $n\varphi - 0 = 2\pi k$ pour un entier k, par suite, $\varphi = \frac{2\pi k}{n}$. En outre, en vertu de (1), $0 \leqslant \varphi = \frac{2\pi k}{n} < 2\pi$ et, partant, $0 \leqslant k < n$. Donc,

$$w = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n} = w_k \in \{w_0, w_1, \ldots, w_{n-1}\}. \ \square$$

COROLLAIRE 8.6. *Les points du plan complexe représentant les racines n-ièmes de l'unité occupent les sommets d'un polygone régulier à n angles inscrit dans le cercle de rayon unité et de centre à l'origine des coordonnées, de plus, l'un des sommets se trouve au point* (0, 1).

DÉFINITION. Le nombre complexe w est appelé *racine primitive n-ième de l'unité* ($n \geqslant 1$) si l'ensemble des nombres $\{w^0, w^1, \ldots, w^{n-1}\}$ constitue un ensemble de toutes les solutions de l'équation $z^n = 1$.

C'est ainsi, par exemple, que pour tout $n \geqslant 1$ naturel le nombre $w_1 = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$ est, en vertu du théorème 8.5, la racine primitive n-ième de l'unité.

Racines n-ièmes d'un nombre complexe arbitraire. La forme trigonométrique d'un nombre complexe résout totalement le problème de l'extraction des racines des nombres complexes.

THÉORÈME 8.7. *Soient* $c = |c| (\cos\varphi + i \sin\varphi)$ *un nombre complexe différent de zéro et n un nombre naturel non nul. Il y a n racines n-ièmes distinctes du nombre c et, toutes, elles s'obtiennent à l'aide de la formule*

$$u_k = |c|^{1/n} \left(\cos\frac{\varphi + 2\pi k}{n} + i \sin\frac{\varphi + 2\pi k}{n}\right), \quad k = 0, 1, \ldots, n-1.$$

Démonstration. Montrons qu'on a

(1) $u_k = u_0 w_k, \quad k = 0, 1, \ldots, n-1,$

où $w_0, \ldots, w_{n-1}$ sont les racines n-ièmes de l'unité et

$$u_0 = |c|^{1/n}\left(\cos\frac{\varphi}{n} + i\sin\frac{\varphi}{n}\right).$$

En effet, en vertu de la formule de Moivre

$$u_k = |c|^{1/n}\left(\cos\frac{\varphi}{n} + i\sin\frac{\varphi}{n}\right)\left(\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}\right) = u_0 w_k.$$

Chacun des nombres u_k est une racine n-ième du nombre c, car, en vertu de (1),

$$u_k^n = u_0^n w_k^n = u_0^n = (|c|^{1/n})^n\left(\cos\frac{\varphi}{n} + i\sin\frac{\varphi}{n}\right)^n =$$
$$= |c|(\cos\varphi + i\sin\varphi) = c.$$

Si u est une racine n-ième arbitraire du nombre c, alors $(uu_0^{-1})^n = u^n(u_0^n)^{-1} = cc^{-1} = 1$. Donc,

$$uu_0^{-1} \in \{w_0, \ldots, w_{n-1}\}$$

et en vertu de (1)

$$u \in \{u_0 w_0, \ldots, u_0 w_{n-1}\} = \{u_0, \ldots, u_{n-1}\}.$$

Par conséquent, l'ensemble $\{u_0, \ldots, u_{n-1}\}$ est l'ensemble de toutes les racines n-ièmes du nombre c. Cet ensemble contient exactement n éléments distincts, vu que

$$\{u_0, \ldots u_{n-1}\} = \{u_0 w_0, \ldots, u_0 w_{n-1}\},$$

$u_0 \neq 0$ et les nombres $w_0, \ldots, w_{n-1}$ diffèrent deux par deux selon le théorème 8.2). □

Exercices

1. Représenter en forme trigonométrique les nombres complexes:

$$1,\ i,\ -1,\ -i,\ 1+i,\ 1-i,\ -\frac{1}{2}+i\frac{\sqrt{3}}{2},\ \sqrt{3}+i.$$

2. Chercher l'ensemble des points du plan représentant les nombres complexes z pour lesquels:

(a) $\arg z = 0$; (b) $\arg z = \frac{\pi}{3}$; (c) $\arg z = \pi$; (d) $\arg z = \frac{\pi}{2}$.

3. A quelles conditions le module de la somme de deux nombres complexes est égal à la somme des modules des termes?

4. A quelles conditions le module de la somme de deux nombres complexes est égal à la différence des modules des termes?

5. Décrire les applications suivantes $(\mathbf{C} \to \mathbf{C})$:

(a) $z \mapsto \bar{z}$; (b) $z \mapsto \frac{1}{z}$ $(z \neq 0)$; (c) $z \mapsto iz$;

(d) $z \mapsto \overline{iz}$; (e) $z \mapsto rz$, où r est un nombre positif;

(f) $z \mapsto (\cos\varphi + i\sin\varphi)$; (g) $z \mapsto -\bar{z}$;

(h) $z \mapsto r(\cos\varphi + i\sin\varphi)$; (i) $z \mapsto \bar{z}^{-1}$.

6. Soient $w = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$ et n un nombre naturel. Calculer: a) $(1+w)^n$; (b) $w^n + \bar{w}^n$.

7. Calculer la somme $\frac{1}{2} + \cos x + \cos 2x + \ldots + \cos nx$.

8. Montrer que $\sin x + \sin 2x + \ldots + \sin nx = \dfrac{\sin\frac{n+1}{2}x \cdot \sin\frac{nx}{2}}{\sin\frac{x}{2}}$.

9. Exprimer à l'aide de $\cos x$ et $\sin x$:

(a) $\cos 5x$; (b) $\sin 5x$; (c) $\cos 6x$; (d) $\sin 6x$; (e) $\cos 8x$.

10. Chercher les formules exprimant $\cos nx$ et $\sin nx$ à l'aide de $\cos x$ et $\sin x$.

11. Exprimer en forme de polynôme trigonométrique du premier degré de cosinus et de sinus d'angles multiples de x:

(a) $\sin^3 x$; (b) $\cos^5 x$; (c) $\sin^5 x$; (d) $\cos^6 x$.

12. Trouver toutes les racines de l'unité d'indice:

(a) 2; (b) 3; (c) 6; (d) 8; (e) 12; (f) 24.

13. Trouver toutes les racines complexes des équations:

(a) $z^3 + i = 0$; (b) $z^3 + 2 + 2i = 0$; (c) $z^4 + \frac{1}{2} + i\frac{\sqrt{3}}{2} = 0$;

(d) $z^6 + i = 0$; (e) $z^5 - 1 = 0$.

14. Trouver la somme et le produit de toutes les racines n-ièmes de 1.

15. Soit $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, où n est un entier positif. Montrer que le nombre complexe z est une racine primitive n-ième de l'unité si et seulement si $z = \varepsilon^m$ pour un nombre naturel m premier avec n.

16. Chercher les racines primitives d'indice:

(a) 2; (b) 3; (c) 4; (d) 5; (e) 6; (f) 8; (g) 12; (h) 24.

17. Chercher tous les nombres complexes satisfaisant à la condition $\bar{z} = z^{n-1}$, où n est un entier positif et $\bar{z}$ le conjugué de z.

18. Démontrer les affirmations suivantes:

(a) le produit de la racine m-ième de 1 par la racine n-ième de 1 est une racine mn-ième de 1;

(b) si m et n sont premiers entre eux, il n'y a qu'un seul nombre complexe z satisfaisant aux conditions $z^m = 1$ et $z^n = 1$;

(c) si les nombres m et n sont premiers entre eux, toutes les racines mn-ièmes de 1 s'obtiennent alors par multiplication des racines m-ièmes de 1 par les racines n-ièmes de 1;

(d) si m et n sont premiers entre eux, le produit de la racine primitive m-ième de 1 par la racine primitive n-ième de 1 est alors une racine primitive mn-ième de 1 et réciproquement.

CHAPITRE V

ESPACES VECTORIELS ARITHMÉTIQUES ET SYSTÈMES D'ÉQUATIONS LINÉAIRES

§ 1. Espaces vectoriels arithmétiques

Espace vectoriel arithmétique à n dimensions. Soient $\mathcal{F}$ un corps de choix arbitraire, $\mathcal{F} = \langle F, +, -, \cdot, 1 \rangle$, et F son ensemble de base. Les éléments de l'ensemble F sont appelés scalaires, F l'ensemble des scalaires et $\mathcal{F}$ le corps des scalaires. Soit n un nombre naturel fixé autre que zéro.

DÉFINITION. On appelle *vecteur à n dimensions sur le corps $\mathcal{F}$* tout cortège de n éléments du corps $\mathcal{F}$. L'ensemble de tous les vecteurs à n dimensions sur le corps $\mathcal{F}$ est noté par le symbole F^n.

Généralement le vecteur est présenté sous forme d'une ligne ou d'une colonne. Dans ce paragraphe on écrira le vecteur à n dimensions en ligne

$$(\alpha_1 \ \alpha_2, \ldots, \alpha_n),$$

où $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$.

Introduisons sur l'ensemble des vecteurs à n dimensions sur le corps $\mathcal{F}$ la relation d'égalité, l'opération d'addition des vecteurs et l'opération de multiplication du vecteur par un scalaire.

DÉFINITION. Les vecteurs $(\alpha_1, \ldots, \alpha_n)$ et $(\beta_1, \ldots, \beta_n)$ sont dits *égaux* si $\alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n$.

DÉFINITION. On appelle *somme des vecteurs* $(\alpha_1, \ldots, \alpha_n)$ et $(\beta_1, \ldots, \beta_n)$ le vecteur $(\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$, c'est-à-dire

$$(\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n).$$

DÉFINITION. On appelle *produit d'un scalaire λ par le vecteur* $(\alpha_1, \ldots, \alpha_n)$ le vecteur $(\lambda\alpha_1, \ldots, \lambda\alpha_n)$, c'est-à-dire

$$\lambda (\alpha_1, \ldots, \alpha_n) = (\lambda\alpha_1, \ldots, \lambda\alpha_n).$$

L'opération de multiplication par un scalaire λ sera désignée par le symbole ω_λ, c'est-à-dire

$$\omega_\lambda (\alpha_1, \ldots, \alpha_n) = \lambda (\alpha_1, \ldots, \alpha_n).$$

Pour chaque λ de F, ω_λ est une opération singulaire sur l'ensemble F^n des vecteurs à n dimensions.

Le vecteur $(0, \ldots, 0)$ est appelé *vecteur nul* et noté **0**. Un vecteur nul est un élément neutre par rapport à l'addition.

Le vecteur $(-1)\cdot(\alpha_1, \ldots, \alpha_n)$ est dit *vecteur opposé du vecteur* $\mathbf{a} = (\alpha_1, \ldots, \alpha_n)$ et est noté $-\mathbf{a}$. Il va de soi que $\mathbf{a} + (-\mathbf{a}) = \mathbf{0}$.

DÉFINITION. On appelle *espace vectoriel arithmétique à n dimensions sur le corps* $\mathcal{F}$ l'ensemble F^n associé à l'opération binaire d'addition et aux opérations singulaires ω_λ, autrement dit, l'algèbre $\langle F^n, +, \{\omega_\lambda \mid \lambda \in F\}\rangle$.

L'espace vectoriel arithmétique à n dimensions sur le corps $\mathcal{F}$ est désigné par le symbole $\mathcal{F}^n$.

L'opération d'addition des vecteurs et les opérations singulaires ω_λ sont les opérations principales de l'espace vectoriel $\mathcal{F}^n$.

THÉORÈME 1.1. *Les opérations principales de l'espace vectoriel* $\mathcal{F}^n$ *sont douées des propriétés suivantes:*

(1) *l'algèbre* $\langle F^n, +, -\rangle$, *où* $-\mathbf{a} = \omega_{-1}(\mathbf{a})$ *pour tout* $\mathbf{a}$ *de* F^n, *est un groupe abélien;*

(2) *la multiplication par des scalaires est associative, c'est-à-dire que* $(\alpha\beta)\,\mathbf{a} = \alpha\,(\beta\mathbf{a})$ *pour tous* α, β *de* F *et tout* $\mathbf{a}$ *de* F^n;

(3) *la multiplication par un scalaire est distributive par rapport à l'addition, c'est-à-dire que* $\alpha\,(\mathbf{a} + \mathbf{b}) = \alpha\mathbf{a} + \alpha\mathbf{b}$ *pour tout* α *de* F *et tous* $\mathbf{a}$, $\mathbf{b}$ *de* F^n;

(4) *la multiplication par un vecteur est distributive par rapport à l'addition des scalaires, c'est-à-dire que* $(\alpha + \beta)\,\mathbf{a} = \alpha\mathbf{a} + \beta\mathbf{a}$ *pour tous* α, β *de* F *et tout* $\mathbf{a}$ *de* F^n;

(5) $1\cdot\mathbf{a} = \mathbf{a}$ *pour tout* $\mathbf{a}$ *de* F^n.

D é m o n s t r a t i o n. Démontrons que l'algèbre $\langle F^n, +, -\rangle$ est un groupe commutatif. La commutativité de l'addition des vecteurs découle directement de la définition de l'addition, ainsi que du fait que $\mathcal{F}$ est un corps. L'associativité de l'addition s'ensuit de l'associativité de l'addition des scalaires:

$$
\begin{aligned}
(\mathbf{a} + \mathbf{b}) + \mathbf{c} &= ((\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n)) + (\gamma_1, \ldots, \gamma_n) = \\
&= (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n) + (\gamma_1, \ldots, \gamma_n) = \\
&= ((\alpha_1 + \beta_1) + \gamma_1, \ldots, (\alpha_n + \beta_n) + \gamma_n) = \\
&= (\alpha_1 + (\beta_1 + \gamma_1), \ldots, \alpha_n + (\beta_n + \gamma_n)) = \\
&= (\alpha_1, \ldots, \alpha_n) + (\beta_1 + \gamma_1, \ldots, \beta_n + \gamma_n) = \\
&= \mathbf{a} + (\mathbf{b} + \mathbf{c}).
\end{aligned}
$$

Le vecteur **0** est un élément neutre par rapport à l'addition, c'est-à-dire que $\mathbf{a} + \mathbf{0} = \mathbf{0} + \mathbf{a} = \mathbf{a}$ pour tout vecteur **a**. Le vecteur $-\mathbf{a} = (-\alpha_1, \ldots, -\alpha_n)$ est l'opposé du vecteur **a**, c'est-à-dire que $\mathbf{a} + (-\mathbf{a}) = \mathbf{0} = (-\mathbf{a}) + \mathbf{a}$. $\langle F^n, +, -\rangle$ est donc un groupe. Sa commutativité se déduit de la commutativité de l'addition des scalaires.

On vérifie de même sans peine la validité des propriétés (2)-(5). □

Dépendance et indépendance linéaires d'un système de vecteurs. Soient $\mathcal{F}$ un corps des scalaires et F son ensemble de base. Soient $\mathcal{V} = \mathcal{F}^n$ un espace vectoriel arithmétique à n dimensions sur $\mathcal{F}$ et $\mathbf{a}_1, \ldots, \mathbf{a}_m$ un système quelconque de vecteurs de l'espace $\mathcal{V}$.

DÉFINITION. On appelle *combinaison linéaire du système des vecteurs* $\mathbf{a}_1, \ldots, \mathbf{a}_m$ une somme de la forme $\lambda_1\mathbf{a}_1 + \ldots + \lambda_m\mathbf{a}_m$, où $\lambda_1, \ldots, \lambda_m \in F$. Les scalaires $\lambda_1, \ldots, \lambda_m$ sont dits *coefficients de la combinaison linéaire*. Une combinaison linéaire est dite *non triviale* si au moins un de ses coefficients est différent de zéro. Elle est, par contre, dite *triviale* si tous ses coefficients sont nuls.

DÉFINITION. L'ensemble de toutes les combinaisons linéaires des vecteurs du système $\mathbf{a}_1, \ldots, \mathbf{a}_m$ est nommé *enveloppe linéaire* de ce système et noté $L(\mathbf{a}_1, \ldots, \mathbf{a}_m)$. L'enveloppe linéaire d'un système vide est un ensemble composé du vecteur nul.

Bref, par définition,

$$L(\mathbf{a}_1, \ldots, \mathbf{a}_m) = \{\lambda_1\mathbf{a}_1 + \lambda_2\mathbf{a}_2 + \ldots + \lambda_m\mathbf{a}_m \mid \lambda_1, \ldots, \lambda_m \in F\}.$$

On constate sans peine que l'enveloppe linéaire d'un système donné des vecteurs est fermée relativement aux opérations d'addition des vecteurs et de multiplication des vecteurs par des scalaires.

DÉFINITION. Un système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ est dit *linéairement indépendant* (ou libre) si pour des scalaires quelconques $\lambda_1, \ldots, \lambda_m$ de l'égalité $\lambda_1\mathbf{a}_1 + \ldots + \lambda_m\mathbf{a}_m = \mathbf{0}$ s'ensuivent les égalités $\lambda_1 = 0, \ldots, \lambda_m = 0$. Un système des vecteurs vide est dit linéairement indépendant.

Autrement dit, un système des vecteurs fini est linéairement indépendant si et seulement si toute combinaison linéaire non triviale des vecteurs du système n'est pas égale au vecteur nul.

DÉFINITION. Un système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ est dit *linéairement dépendant* (ou lié) s'il existe des scalaires $\lambda_1, \ldots, \lambda_m$ non tous nuls, tels que

$$\lambda_1\mathbf{a}_1 + \ldots + \lambda_m\mathbf{a}_m = \mathbf{0}.$$

Autrement dit, un système des vecteurs fini est dit linéairement dépendant (lié) s'il existe une combinaison linéaire non triviale des vecteurs du système égale au vecteur nul.

Le système des vecteurs

$$\mathbf{e}_1 = (1, 0, \ldots, 0), \quad \mathbf{e}_2 = (0, 1, 0, \ldots, 0), \ldots, \quad \mathbf{e}_n = (0, 0, \ldots, 0, 1)$$

est appelé *système des vecteurs unités* de l'espace vectoriel $\mathcal{F}^n$. Ce système des vecteurs est linéairement indépendant. En effet, pour tous scalaires $\lambda_1, \ldots, \lambda_n$ de l'égalité $\lambda_1\mathbf{e}_1 + \ldots + \lambda_n\mathbf{e}_n = \mathbf{0}$ on a l'égalité $(\lambda_1, \ldots, \lambda_n) = \mathbf{0}$ et, partant, les égalités $\lambda_1 = 0, \ldots, \lambda_n = 0$.

Examinons les propriétés de dépendance et indépendance linéaires d'un système des vecteurs.

PROPRIETE 1.1. *Un système des vecteurs comportant un vecteur nul est linéairement dépendant.*

Démonstration. Si dans le système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_k, \ldots, \mathbf{a}_m$ un des vecteurs, par exemple le vecteur $\mathbf{a}_k$, est nul, la combinaison linéaire des vecteurs du système, dont tous les coefficients sont nuls, excepté le coefficient associé à $\mathbf{a}_k$, est alors égale au vecteur nul. Par conséquent, un tel système des vecteurs est linéairement dépendant. □

PROPRIETE 1.2. *Un système des vecteurs est linéairement dépendant si un de ses sous-systèmes est linéairement dépendant.*

Démonstration. Soit $\mathbf{a}_1, \ldots, \mathbf{a}_k$ un sous-système linéairement dépendant appartenant au système $\mathbf{a}_1, \ldots, \mathbf{a}_m$, c'est-à-dire qu'on a $\lambda_1\mathbf{a}_1 + \ldots + \lambda_k\mathbf{a}_k = \mathbf{0}$ avec au moins un des coefficients de $\lambda_1, \lambda_2, \ldots, \lambda_k$ différent de zéro. Alors, $\lambda_1\mathbf{a}_1 + \ldots + \lambda_k\mathbf{a}_k + 0\cdot\mathbf{a}_{k+1} + \ldots + 0\cdot\mathbf{a}_m = \mathbf{0}$. Donc, le système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ est linéairement dépendant. □

COROLLAIRE. *Tout sous-système du système linéairement indépendant est lui-même linéairement indépendant.*

PROPRIETE 1.3. *Le système des vecteurs*

$$(1) \qquad \mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m,$$

dans lequel $\mathbf{u}_1 \neq \mathbf{0}$ *est linéairement dépendant si et seulement si au moins un des vecteurs* $\mathbf{u}_2, \ldots, \mathbf{u}_m$ *constitue une combinaison linéaire des vecteurs susmentionnés.*

Démonstration. Soit le système (1) linéairement dépendant et $\mathbf{u}_1 \neq \mathbf{0}$. Il existe dans ce cas des scalaires $\lambda_1, \ldots, \lambda_m$ non tous nuls, tels que

$$(2) \qquad \lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m = \mathbf{0}.$$

Notons k le plus grand des nombres $1, 2, \ldots, m$ satisfaisant à la condition $\lambda_k \neq 0$. On peut alors écrire l'égalité (2) sous la forme

$$(3) \qquad \lambda_1\mathbf{u}_1 + \ldots + \lambda_k\mathbf{u}_k = \mathbf{0}.$$

Remarquons que $k > 1$, car dans le cas contraire $\lambda_2 = 0, \ldots, \lambda_m = 0$, $\lambda_1\mathbf{u}_1 = \mathbf{0}$; donc, $\lambda_1 = 0$, vu que $\mathbf{u}_1 \neq \mathbf{0}$. Il s'ensuit de (3) l'égalité

$$\mathbf{u}_k = (-\lambda_k^{-1}\lambda_1)\,\mathbf{u}_1 + \ldots + (-\lambda_k^{-1}\lambda_{k-1})\,\mathbf{u}_{k-1}.$$

Posons maintenant que le vecteur $\mathbf{u}_s$, $1 < s \leqslant m$, est une combinaison linéaire des vecteurs qui le précèdent, c'est-à-dire que $\mathbf{u}_s = \lambda_1\mathbf{u}_1 + \ldots + \lambda_{s-1}\mathbf{u}_{s-1}$. On a alors $\lambda_1\mathbf{u}_1 + \ldots + \lambda_{s-1}\mathbf{u}_{s-1} + (-1)\,\mathbf{u}_s = \mathbf{0}$, autrement dit, le sous-système $\mathbf{u}_1, \ldots, \mathbf{u}_s$ du système (1) est linéairement dépendant. Par conséquent, selon la pro-

priété 1.2, le système de départ (1) est également linéairement dépendant. □

PROPRIÉTÉ 1.4. *Si le système des vecteurs* $\mathbf{u}_1, \ldots, \mathbf{u}_m$ *est linéairement indépendant, tandis que le système des vecteurs*

(2) $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m, \mathbf{v}$

est linéairement dépendant, alors le vecteur $\mathbf{v}$ *peut être exprimé linéairement au moyen des vecteurs*

(1) $\mathbf{u}_1, \ldots, \mathbf{u}_m,$

et cela de façon unique.

Démonstration. Par hypothèse le système (2) est linéairement dépendant, c'est-à-dire qu'il existe des scalaires $\lambda_1, \ldots, \lambda_m$, λ non tous nuls, tels que

(3) $\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m + \lambda\mathbf{v} = \mathbf{0}.$

De plus $\lambda \neq 0$, car pour $\lambda = 0$ $\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m = \mathbf{0}$, ce qui est en contradiction avec l'indépendance linéaire du système (1). De (3) s'ensuit l'égalité

$$\mathbf{v} = (-\lambda^{-1}\lambda_1)\,\mathbf{u}_1 + \ldots + (-\lambda^{-1}\lambda_m)\,\mathbf{u}_m.$$

Si $\mathbf{v} = \lambda'_1\mathbf{u}_1 + \ldots + \lambda'_m\mathbf{u}_m$ et $\mathbf{v} = \mu_1\mathbf{u}_1 + \ldots + \mu_m\mathbf{u}_m$, alors

$$(\lambda'_1 - \mu_1)\,\mathbf{u}_1 + \ldots + (\lambda'_m - \mu_m)\,\mathbf{u}_m = \mathbf{0}.$$

En vertu de l'indépendance linéaire du système (1) il s'ensuit que

$$\lambda'_1 - \mu_1 = 0, \ldots, \lambda'_m - \mu_m = 0 \quad \text{et}$$

$$\lambda'_1 = \mu_1, \ldots, \lambda'_m = \mu_m. \ \square$$

PROPRIÉTÉ 1.5. *Si* $\mathbf{u} \in L(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m)$ *et* $\mathbf{v}_1, \ldots, \mathbf{v}_m \in L(\mathbf{w}_1, \ldots, \mathbf{w}_s)$, *on a alors* $\mathbf{u} \in L(\mathbf{w}_1, \ldots, \mathbf{w}_s)$.

Démonstration. La condition $\mathbf{u} \in L(\mathbf{v}_1, \ldots, \mathbf{v}_m)$ signifie qu'il existe des scalaires $\alpha_1, \ldots, \alpha_m$, tels que

(1) $\mathbf{u} = \alpha_1\mathbf{v}_1 + \ldots + \alpha_m\mathbf{v}_m.$

La condition $\mathbf{v}_i \in L(\mathbf{w}_1, \ldots, \mathbf{w}_s)$ signifie qu'il y a des scalaires λ_{ik}, tels que

(2) $\mathbf{v}_i = \lambda_{i1}\mathbf{w}_1 + \ldots + \lambda_{is}\mathbf{w}_s \quad (i = 1, \ldots, m).$

En vertu de (1) et (2), il vient

$$\mathbf{u} = \alpha_1(\lambda_{11}\mathbf{w}_1 + \ldots + \lambda_{1s}\mathbf{w}_s) + \ldots + \alpha_m(\lambda_{m1}\mathbf{w}_1 + \ldots$$
$$\ldots + \lambda_{ms}\mathbf{w}_s) = (\alpha_1\lambda_{11} + \ldots + \alpha_m\lambda_{m1})\,\mathbf{w}_1 + \ldots$$
$$\ldots + (\alpha_1\lambda_{1s} + \ldots + \alpha_m\lambda_{ms})\,\mathbf{w}_s,$$

c'est-à-dire que $\mathbf{u} \in L(\mathbf{w}_1, \ldots, \mathbf{w}_s)$. □

THÉORÈME 1.2. *Si l'on a*

$$(1)\qquad \mathbf{u}_1, \ldots, \mathbf{u}_{m+1} \in L(\mathbf{v}_1, \ldots, \mathbf{v}_m),$$

le système des vecteurs $\mathbf{u}_1, \ldots, \mathbf{u}_{m+1}$ *est alors linéairement dépendant.*

Démonstration (s'effectue par récurrence sur m). Supposons que les vecteurs $\mathbf{u}_1, \ldots, \mathbf{u}_{m+1}$ ne sont pas nuls, car dans le cas contraire le théorème devient évident. Posons $m = 1$ et $\mathbf{u}_1, \mathbf{u}_2 \in L(\mathbf{v}_1)$, c'est-à-dire que $\mathbf{u}_1 = \alpha\mathbf{v}_1$ et $\mathbf{u}_2 = \beta\mathbf{v}_1$. Alors $\alpha \neq 0$, $\beta \neq 0$ et $\alpha^{-1}\mathbf{u}_1 + (-\beta^{-1})\,\mathbf{u}_2 = \mathbf{0}$. Par conséquent, le système des vecteurs $\mathbf{u}_1, \mathbf{u}_2$ est linéairement dépendant.

Supposons que le théorème est vrai pour $m = n - 1$ et démontrons que dans ce cas il se vérifie pour $m = n$. Soit $\mathbf{u}_1, \ldots, \mathbf{u}_{n+1} \in L(\mathbf{v}_1, \ldots, \mathbf{v}_n)$, c'est-à-dire que

$$(2)\qquad \begin{aligned} \mathbf{u}_1 &= \lambda_{11}\mathbf{v}_1 + \ldots + \lambda_{1n}\mathbf{v}_n;\\ &\ldots\ldots\ldots\ldots\\ \mathbf{u}_n &= \lambda_{n1}\mathbf{v}_1 + \ldots + \lambda_{nn}\mathbf{v}_n;\\ \mathbf{u}_{n+1} &= \lambda_{n+1,\,1}\mathbf{v}_1 + \ldots + \lambda_{n+1,\,n}\mathbf{v}_n. \end{aligned}$$

Si dans les seconds membres des égalités (2) tous les coefficients associés à $\mathbf{v}_n$ sont nuls, on a alors $\mathbf{u}_1, \ldots, \mathbf{u}_n \in L(\mathbf{v}_1, \ldots, \mathbf{v}_{n-1})$ et suivant l'hypothèse de récurrence le système des vecteurs $\mathbf{u}_1, \ldots, \mathbf{u}_n$ est linéairement dépendant et, partant, l'est le système $\mathbf{u}_1, \ldots, \mathbf{u}_n, \mathbf{u}_{n+1}$. Mais si au moins un des coefficients associés à $\mathbf{v}_n$, par exemple $\lambda_{n+1,\,n}$, est différent de zéro, on exclut alors le vecteur $\mathbf{v}_n$ des n premières égalités. Et l'on aboutit ainsi à

$$\begin{aligned} \mathbf{u}_1 - \beta_1\mathbf{u}_{n+1} &= \lambda'_{11}\mathbf{v}_1 + \ldots + \lambda'_{1,\,n-1}\mathbf{v}_{n-1};\\ &\ldots\ldots\ldots\ldots\\ \mathbf{u}_n - \beta_n\mathbf{u}_{n+1} &= \lambda'_{n1}\mathbf{v}_1 + \ldots + \lambda'_{n,\,n-1}\mathbf{v}_{n-1}. \end{aligned}$$

Suivant l'hypothèse de récurrence il s'ensuit de (3) que le système des vecteurs $\mathbf{u}_1 - \beta_1\mathbf{u}_{n+1}, \ldots, \mathbf{u}_n - \beta_n\mathbf{u}_{n+1}$ est linéairement dépendant. Il existe donc des scalaires $\lambda_1, \ldots, \lambda_n$ non tous nuls, tels que

$$\lambda_1(\mathbf{u}_1 - \beta_1\mathbf{u}_{n+1}) + \ldots + \lambda_n(\mathbf{u}_n - \beta_n\mathbf{u}_{n+1}) = \mathbf{0}$$

ou

$$\lambda_1\mathbf{u}_1 + \ldots + \lambda_n\mathbf{u}_n + \lambda_{n+1}\mathbf{u}_{n+1} = \mathbf{0},$$

où $\lambda_{n+1} = -(\lambda_1\beta_1 + \ldots + \lambda_n\beta_n)$. Par conséquent, le système des vecteurs $\mathbf{u}_1, \ldots, \mathbf{u}_{n+1}$ est linéairement dépendant. □

COROLLAIRE 1.3. *Si* $\mathbf{u}_1, \ldots, \mathbf{u}_k \in L(\mathbf{v}_1, \ldots, \mathbf{v}_m)$ *et* $k > m$, *alors le système des vecteurs* $\mathbf{u}_1, \ldots, \mathbf{u}_k$ *est linéairement dépendant.*

COROLLAIRE 1.4. *Si* $\mathbf{u}_1, \ldots, \mathbf{u}_k \in L(\mathbf{v}_1, \ldots, \mathbf{v}_m)$ *et le système des vecteurs* $\mathbf{u}_1, \ldots, \mathbf{u}_k$ *est linéairement indépendant, on a alors* $k \leqslant m$.

COROLLAIRE 1.5. *Dans un espace vectoriel arithmétique à n dimen-*

sions tout système composé de $n + 1$ ou plus de vecteurs est linéairement dépendant.

Le corollaire 1.5 découle du théorème 1.2 vu que tout vecteur $(\alpha_1, \ldots, \alpha_n)$ à n dimensions est une combinaison linéaire de vecteurs unités $\mathbf{e}_1, \ldots, \mathbf{e}_n$:

$$(\alpha_1, \ldots, \alpha_n) = \alpha_1\mathbf{e}_1 + \ldots + \alpha_n\mathbf{e}_n \in L(\mathbf{e}_1, \ldots, \mathbf{e}_n).$$

Systèmes des vecteurs équivalents. Introduisons sur un ensemble des systèmes finis des vecteurs d'un espace vectoriel donné V l'opération binaire $\sim$.

DÉFINITION. Soient S et T des systèmes des vecteurs; $S \sim T$ si chaque vecteur non nul d'un quelconque de ces systèmes peut être représenté sous forme d'une combinaison linéaire de vecteurs de l'autre système.

On vérifie sans peine que la relation binaire $\sim$ est réflexive, transitive et symétrique et, par suite, est une relation d'équivalence. C'est pourquoi les systèmes de vecteurs S et T sont dits *équivalents* si $S \sim T$. Notons qu'un système des vecteurs vide est équivalent aussi bien à un système des vecteurs vide qu'à un système composé de vecteurs nuls.

Considérons quelques propriétés de systèmes équivalents des vecteurs.

THÉORÈME 1.6. *Deux systèmes des vecteurs sont équivalents si et seulement si leurs enveloppes linéaires sont égales.*

Démonstration. Soit $S \sim T$. Chaque vecteur du système S appartient alors à l'ensemble $L(T)$, tandis que chaque vecteur du système T appartient à l'ensemble $L(S)$. Aussi en vertu de la propriété 1.5 $L(S) \subset L(T)$ et $L(T) \subset L(S)$, c'est-à-dire $L(S) = L(T)$.

Réciproquement : si $L(S) = L(T)$, on a évidemment $S \sim T$. □

THÉORÈME 1.7. *Si deux systèmes finis des vecteurs sont équivalents et chacun d'eux est linéairement indépendant, alors les deux systèmes sont composés d'un même nombre de vecteurs.*

Démonstration. Le théorème est évidemment vrai si les deux systèmes des vecteurs sont vides. Soient $\mathbf{u}_1, \ldots, \mathbf{u}_r$ et $\mathbf{v}_1, \ldots, \mathbf{v}_s$ deux systèmes équivalents non vides, chacun étant linéairement indépendant. Dans ce cas, en vertu du corollaire 1.4, $r \leqslant s$ et $s \leqslant r$. Donc, $r = s$. □

DÉFINITION. On appelle *transformations élémentaires du système fini des vecteurs* les transformations suivantes :

(α) la multiplication d'un vecteur quelconque du système par un scalaire non nul ;

(β) l'addition (la soustraction) à un des vecteurs du système d'un autre vecteur du système multiplié par un scalaire ;

(γ) l'exclusion du système ou l'inclusion dans le système d'un vecteur nul.

Les transformations élémentaires (α) et (β) sont dites *régulières* et la transformation (γ) est nommée *singulière*.

THÉORÈME 1.8. *Si l'un des systèmes finis des vecteurs s'obtient de l'autre système des vecteurs après une série de transformations élémentaires, ces deux systèmes sont équivalents.*

Démonstration. Soit

(1) $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m$

le système des vecteurs de départ. Si l'on multiplie un des vecteurs du système, par exemple le premier, par un scalaire λ différent de zéro, on obtient le système $\lambda\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m$ équivalent au système de départ.

Si l'on ajoute à l'un des vecteurs du système un autre vecteur multiplié par un scalaire, par exemple, par addition au premier vecteur d'un vecteur k-ième multiplié par λ, on obtient un système $\mathbf{a}_1 + \lambda\mathbf{a}_k, \mathbf{a}_2, \ldots, \mathbf{a}_m$ équivalent au système de départ.

En appliquant au système des vecteurs de départ la transformation (γ), on aboutit apparemment au système des vecteurs équivalent au système de départ. Par suite, en vertu de la transitivité de la relation d'équivalence, le système des vecteurs, obtenu du système (1) par la série des transformations élémentaires, est équivalent au système des vecteurs de départ (1). □

Base d'un système fini des vecteurs. Introduisons une des notions fondamentales de la théorie des espaces vectoriels.

DÉFINITION. On appelle *base d'un système fini des vecteurs* son sous-système non vide linéairement indépendant qui lui est équivalent.

Autrement dit, la base d'un système des vecteurs est son sous-système non vide linéairement indépendant au moyen des vecteurs duquel s'exprime linéairement chacun des vecteurs du système donné.

THÉORÈME 1.9. *Un système fini des vecteurs comportant au moins un vecteur non nul possède une base. Toutes deux bases d'un système des vecteurs fini donné sont composées d'un même nombre de vecteurs.*

Démonstration. Soit donné le système des vecteurs

(1) $\mathbf{u}_1, \ldots, \mathbf{u}_k, \ldots, \mathbf{u}_m,$

comportant un vecteur non nul. Les vecteurs nuls peuvent être exclus du système (1), car le système ainsi obtenu est équivalent à celui de départ. On peut donc considérer que $\mathbf{u}_1 \neq \mathbf{0}$. Si le système (1) est linéairement indépendant, c'est une base du système.

Si le système (1) est linéairement dépendant, alors, en vertu de la propriété 1.3, il existe un vecteur, par exemple le vecteur $\mathbf{u}_k$, égal à la combinaison linéaire des vecteurs qui le précèdent. Par conséquent, le sous-système

(2) $\mathbf{u}_1, \ldots, \mathbf{u}_{k-1}, \mathbf{u}_{k+1}, \ldots, \mathbf{u}_m$

est équivalent au système de départ et possède un vecteur non nul. Si le système (2) est linéairement indépendant, il est une base du système (1). Mais si le système (2) est linéairement dépendant, on peut en exclure le vecteur constituant une combinaison linéaire des vecteurs qui le précèdent, etc. Après un nombre fini d'éliminations, on aboutit à un sous-système des vecteurs dont aucun ne peut être exprimé linéairement au moyen des vecteurs précédents; ce sous-système est la base du système (1), car il est linéairement indépendant et n'est pas vide (contient le vecteur $\mathbf{u}_1$).

Soient $\mathbf{v}_1, \ldots, \mathbf{v}_r$ et $\mathbf{w}_1, \ldots, \mathbf{w}_s$ deux bases du système des vecteurs (1). Ces bases sont équivalentes, car chacune d'elles est équivalente au système (1). Par conséquent, suivant le théorème 1.7, ces bases sont composées d'un même nombre de vecteurs, c'est-à-dire que $r = s$. □

Rang d'un système fini des vecteurs. Introduisons maintenant la notion de rang d'un système des vecteurs.

DÉFINITION. On appelle *rang d'un système fini des vecteurs* le nombre de vecteurs inclus dans une base quelconque du système. Le rang d'un système des vecteurs nuls et le rang d'un système des vecteurs vide sont égaux à zéro.

Considérons quelques propriétés du rang d'un système des vecteurs.

THÉORÈME 1.10. *Si* $\mathbf{u}_1, \ldots, \mathbf{u}_k \in L(\mathbf{v}_1, \ldots, \mathbf{v}_m)$, *le rang du système des vecteurs* $\mathbf{u}_1, \ldots, \mathbf{u}_k$ *est inférieur ou égal au rang du système des vecteurs* $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$.

Démonstration. Si le premier système $\mathbf{u}_1, \ldots, \mathbf{u}_k$ est composé de vecteurs nuls, son rang est alors égal à zéro et ne dépasse donc pas celui du second système $\mathbf{v}_1, \ldots, \mathbf{v}_m$. Supposons que le premier système comporte au moins un vecteur non nul. Alors par hypothèse, il s'ensuit que le second système possède également des vecteurs non nuls. Donc, selon le théorème 1.9, ces systèmes ont chacun une base. Supposons que $\mathbf{u}_1, \ldots, \mathbf{u}_r$ est la base du premier système, tandis que $\mathbf{v}_1, \ldots, \mathbf{v}_s$ la base du second système. Mais alors le système $\mathbf{v}_1, \ldots, \mathbf{v}_s$ est équivalent au système $\mathbf{v}_1, \ldots, \mathbf{v}_m$ et, en vertu du théorème 1.6,

$$L(\mathbf{v}_1, \ldots, \mathbf{v}_m) = L(\mathbf{v}_1, \ldots, \mathbf{v}_s).$$

En outre, par hypothèse, $\mathbf{u}_1, \ldots, \mathbf{u}_k \in L(\mathbf{v}_1, \ldots, \mathbf{v}_m)$, aussi a-t-on $\mathbf{u}_1, \ldots, \mathbf{u}_r \in L(\mathbf{v}_1, \ldots, \mathbf{v}_s)$.

Selon le corollaire 1.4 et en vertu de l'indépendance linéaire du système des vecteurs $\mathbf{u}_1, \ldots, \mathbf{u}_r$ il s'ensuit que $r \leqslant s$. Donc, le rang du premier système des vecteurs n'est pas supérieur à celui du second système. □

PROPOSITION 1.11. *Le rang de tout sous-système du système fini des vecteurs n'est pas supérieur au rang du système entier.*

D é m o n s t r a t i o n. Cette affirmation est évidemment vraie si le sous-système est vide. Si le sous-système n'est pas vide, la proposition 1.11 découle directement du théorème 1.10. □

PROPOSITION 1.12. *Des systèmes finis équivalents des vecteurs ont un même rang.*

Cette proposition découle du théorème 1.10.

PROPOSITION 1.13. *Le rang de tout système fini des vecteurs d'un espace vectoriel arithmétique à n dimensions est inférieur à n.*

D é m o n s t r a t i o n. Soient $\mathbf{e}_1, \ldots, \mathbf{e}_n$ les vecteurs unités de l'espace vectoriel arithmétique $\mathcal{F}^n$. Tout système $\mathbf{a}_1, \ldots, \mathbf{a}_m$ des vecteurs de cet espace est contenu dans l'enveloppe linéaire des vecteurs unitaires $\mathbf{a}_1, \ldots, \mathbf{a}_m \in L(\mathbf{e}_1, \ldots, \mathbf{e}_n) = F^n$. Donc, en vertu du théorème 1.10, le rang du système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ ne peut dépasser n. □

PROPOSITION 1.14. *Si un système fini des vecteurs possède le rang r, tout sous-système de ce dernier composé de k vecteurs avec $k > r$ est alors linéairement dépendant.*

D é m o n s t r a t i o n. Cette affirmation est apparemment vraie si le système est composé de vecteurs nuls. Posons que $\mathbf{v}_1, \ldots, \mathbf{v}_m$ soit un système des vecteurs donné, $\mathbf{v}_1, \ldots, \mathbf{v}_r$ sa base, $\mathbf{u}_1, \ldots, \mathbf{u}_k$ le sous-système du système donné; on a alors

$$\mathbf{u}_1, \ldots, \mathbf{u}_k \in L(\mathbf{v}_1, \ldots, \mathbf{v}_r) = L(\mathbf{v}_1, \ldots, \mathbf{v}_m).$$

En vertu du corollaire 1.3 pour $k > r$ il s'ensuit que le système des vecteurs $\mathbf{u}_1, \ldots, \mathbf{u}_k$ est linéairement dépendant. □

PROPOSITION 1.15. *Supposons que le rang du système des vecteurs*

$$(1) \qquad \mathbf{a}_1, \ldots, \mathbf{a}_m$$

soit égal au rang du système des vecteurs

$$(2) \qquad \mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}.$$

On peut alors représenter le vecteur **b** *sous forme d'une combinaison linéaire des vecteurs du système* (1).

D é m o n s t r a t i o n. La proposition est évidemment vraie si les rangs des systèmes (1) et (2) sont égaux à zéro. Supposons que le rang r du système (1) est différent de zéro et $\mathbf{a}_1, \ldots, \mathbf{a}_r$ est la base du système (1). Comme, par hypothèse, le rang du système (2) est aussi égal à r, son sous-système $\mathbf{a}_1, \ldots, \mathbf{a}_r, \mathbf{b}$ est linéairement dépendant. Il s'ensuit, en vertu du corollaire 1.4, que $\mathbf{b} \in L(\mathbf{a}_1, \ldots, \mathbf{a}_r)$. Donc, $\mathbf{b} \in L(\mathbf{a}_1, \ldots, \mathbf{a}_m)$, autrement dit, il existe des scalaires $\lambda_1, \ldots, \lambda_m$ tels que

$$\mathbf{b} = \lambda_1\mathbf{a}_1 + \ldots + \lambda_m\mathbf{a}_m. \quad \square$$

Exercices

1. Soient (α, β) et (γ, δ) des vecteurs de l'espace $\mathcal{F}^2$. Montrer que ces vecteurs sont linéairement dépendants si et seulement si $\alpha\delta - \beta\gamma = 0$.

2. Montrer que les vecteurs arithmétiques à n dimensions **a** et **b** sont linéairement dépendants si et seulement si **a** et **b** sont proportionnels, c'est-à-dire que pour un scalaire λ on a $\mathbf{a} = \lambda\mathbf{b}$ ou $\mathbf{b} = \lambda\mathbf{a}$.

3. A quelles conditions doivent satisfaire les scalaires β et γ pour que les vecteurs (α, β) et (α, γ) soient linéairement dépendants?

4. Démontrer que si à un système des vecteurs linéairement indépendants $\mathbf{a}_1, \ldots, \mathbf{a}_m$ on adjoint à gauche ou à droite un vecteur quelconque **b**, dans le système obtenu un seul vecteur au maximum s'exprimera linéairement au moyen des vecteurs qui le précèdent.

5. Soient $\mathbf{a}_1, \ldots, \mathbf{a}_m$ et $\mathbf{b}_1, \ldots, \mathbf{b}_m$ deux systèmes des vecteurs linéairement indépendants. Démontrer que si $\mathbf{a}_1, \ldots, \mathbf{a}_m \in L(\mathbf{b}_1, \ldots, \mathbf{b}_m)$, on a alors $\mathbf{b}_1, \ldots, \mathbf{b}_m \in L(\mathbf{a}_1, \ldots, \mathbf{a}_m)$.

6. Soient $\mathcal{F} = \mathcal{Z}_2$ un corps résiduel modulo 2 et $\mathcal{V} = \mathcal{F}^n$. Montrer que $\mathbf{a} + \mathbf{a} = 0$ pour tout vecteur $\mathbf{a} \in V = F^n$.

7. Soient $\mathcal{F} = \mathcal{Z}_3$ un corps des classes résiduelles modulo 3 et $\mathcal{V} = \mathcal{F}^n$. Montrer que $\mathbf{a} + \mathbf{a} + \mathbf{a} = 0$ pour tout vecteur $\mathbf{a} \in V$.

8. Soient $\mathcal{F} = \mathcal{Z}_3$ un corps des classes résiduelles modulo 3 et n un entier positif. Combien de vecteurs contient l'espace vectoriel $\mathcal{F}^n$?

9. Quand un système des vecteurs possède-t-il une base unique?

10. Démontrer que tout sous-système r des vecteurs linéairement indépendants d'un système des vecteurs de rang r est une base du système.

11. Soit $\mathbf{a}_1, \ldots, \mathbf{a}_m$ un système des vecteurs linéairement indépendants. Démontrer que $\mathbf{b} \in L(\mathbf{a}_1, \ldots, \mathbf{a}_m)$ si et seulement si le système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}$ est linéairement dépendant.

12. Démontrer que $\mathbf{b} \in L(\mathbf{a}_1, \ldots, \mathbf{a}_m)$ si et seulement si le rang du système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ est égal à celui du système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}$.

13. Démontrer que deux systèmes des vecteurs non vides équivalents linéairement indépendants renferment le même nombre de vecteurs.

14. Montrer que si deux systèmes des vecteurs ont un même rang et les vecteurs d'un des systèmes s'expriment linéairement en fonction des vecteurs de l'autre, ces deux systèmes sont équivalents.

§ 2. Systèmes d'équations linéaires

Implications du système d'équations linéaires. Partout plus bas $\mathcal{F}$ est un corps, un corps des scalaires.

Définition. On appelle *système d'équations linéaires sur le corps* $\mathcal{F}$ *à variables* $x_1, \ldots, x_n$ le système de la forme

$$\alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = \beta_1,$$
$$\cdots\cdots\cdots\cdots$$
$$\alpha_{m1}x_1 + \ldots + \alpha_{mn}x_n = \beta_m,$$

où $\alpha_{ik}, \beta_i \in F$.

Ce système de m équations linéaires sera noté sous la forme

$$(1) \quad \alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = \beta_i \quad (i = 1, \ldots, m).$$

Le système d'équations linéaires (1) constitue le prédicat (la condition) à n variables libres $x_1, \ldots, x_n$. Les valeurs spécifiées des

variables libres sont considérées partout plus loin comme des éléments du corps des scalaires $\mathcal{F}$. Ce prédicat n-aire est une conjonction de m prédicats n-aires plus simples définis chacun par l'une des équations du système (1).

Définition. Le vecteur $(\xi_1, \ldots, \xi_n)$ de F^n est dit *solution du système d'équations* (1) si sont vraies les égalités

$$\alpha_{i1}\xi_1 + \ldots + \alpha_{in}\xi_n = \beta_i \quad (i = 1, \ldots, m).$$

Définition. Un système d'équations linéaires est dit *compatible* s'il possède au moins une solution. Il est dit *incompatible* s'il est démuni de solutions, c'est-à-dire que l'ensemble de toutes ses solutions est vide.

A côté du système (1) considérons le système (sur $\mathcal{F}$)

$$(2) \qquad \gamma_{i1}x_1 + \ldots + \gamma_{in}x_n = \delta_i \quad (i = 1, \ldots, s).$$

Notons qu'un système d'équations linéaires peut ne comporter qu'une équation.

Définition. Le système d'équations (2) est dit *implication du système d'équations* (1) si chaque solution du système (1) est également une solution du système (2).

La notation (1) $\Rightarrow$ (2) signifie que le système (2) est une implication du système (1).

Tout système d'équations linéaires (sur $\mathcal{F}$) à n variables constitue une implication du système d'équations incompatible (sur $\mathcal{F}$) aux mêmes variables.

Le système d'équations linéaires (2) est une implication du système d'équations (1) si et seulement si l'ensemble de toutes les solutions du système (1) est un sous-ensemble de l'ensemble de toutes les solutions de (2).

On constate sans peine que la relation binaire d'implication sur un ensemble de systèmes d'équations linéaires (sur $\mathcal{F}$) est réflexive et transitive, c'est-à-dire est une relation de préordre.

Définition. L'équation linéaire

$$(\lambda_1\alpha_{11} + \ldots + \lambda_m\alpha_{m1})\,x_1 + \ldots + (\lambda_1\alpha_{1n} + \ldots + \lambda_m\alpha_{mn})\,x_n = \\ = \lambda_1\beta_1 + \ldots + \lambda_m\beta_m,$$

où $\lambda_1, \ldots, \lambda_m$ sont des éléments arbitraires du corps $\mathcal{F}$, est appelée *combinaison linéaire d'équations du système* (1) à coefficients $\lambda_1, \ldots$ $\ldots, \lambda_m$.

Proposition 2.1. *Toute combinaison linéaire d'équations linéaires du système d'équations* (1) *est une implication de ce système.*

La démonstration de cette proposition est laissée au soin du lecteur.

Systèmes équipotents d'équations linéaires et transformations élémentaires du système. On étudie plus loin les systèmes d'équations linéaires sur le corps $\mathcal{F}$ à n variables $x_1, \ldots, x_n$.

DÉFINITION. Deux systèmes d'équations linéaires sont dits *équipotents* si chaque solution de l'un quelconque de ces systèmes est une solution de l'autre système.

Les propositions suivantes établissent les propriétés de l'équipotence découlant de la définition de l'équipotence, ainsi que des propriétés susmentionnées de l'implication des systèmes.

PROPOSITION 2.2. *Deux systèmes d'équations linéaires sont équipotents si et seulement si chacun de ces systèmes est une implication de l'autre système.*

PROPOSITION 2.3. *Deux systèmes d'équations linéaires sont équipotents si et seulement si l'ensemble de toutes les solutions de l'un des systèmes coïncide avec l'ensemble de toutes les solutions de l'autre système.*

PROPOSITION 2.4. *Deux systèmes d'équations linéaires sont équipotents si et seulement si sont équipotents les prédicats définis par ces systèmes.*

DÉFINITION. On appelle *transformations élémentaires d'un système d'équations linéaires* les transformations suivantes:

(α) la multiplication des deux membres d'une équation quelconque du système par un scalaire autre que zéro;

(β) l'addition (la soustraction) aux deux membres d'une équation quelconque du système de membres correspondants d'une autre équation du système multipliés par un scalaire;

(γ) l'élimination du système ou l'adjonction au système d'une équation linéaire à coefficients nuls et à terme libre nul.

THÉORÈME 2.5. *Si un système d'équations linéaires s'obtient d'un autre système d'équations linéaires au bout d'une série de transformations élémentaires, les deux systèmes sont équipotents.*

Démonstration. Soit donné un système

$$(1)\qquad \begin{array}{l} \alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = \beta_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_{m1}x_1 + \ldots + \alpha_{mn}x_n = \beta_m. \end{array}$$

Si l'on multiplie l'une de ses équations, par exemple la première, par un scalaire λ différent de zéro, on obtient le système

$$(2)\qquad \begin{array}{l} \lambda\alpha_{11}x_1 + \ldots + \lambda\alpha_{1n}x_n = \lambda\beta_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_{m1}x_1 + \ldots + \alpha_{mn}x_n = \beta_m. \end{array}$$

Chaque solution du système (1) est également une solution du système (2). Et réciproquement: si $(\xi_1, \ldots, \xi_n)$ est une solution quel-

conque du système (2), c'est-à-dire

$$\lambda\alpha_{11}\xi_1 + \ldots + \lambda\alpha_{1n}\xi_n = \lambda\beta_1,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\alpha_{m1}\xi_1 + \ldots + \alpha_{mn}\xi_n = \beta_m,$$

alors en multipliant la première égalité par λ^{-1} et en ne faisant pas varier les égalités suivantes on obtient des égalités montrant que le vecteur $(\xi_1, \ldots, \xi_n)$ est une solution du système (1). Donc, le système (2) est équipotent au système initial (1). D'une manière aussi aisée on vérifie qu'en appliquant une seule fois au système (1) la transformation élémentaire (β) ou (γ), on aboutit au système équipotent au système initial (1). Vu que la relation d'équipotence est transitive, une application multiple des transformations élémentaires donne un système d'équations équipotent au système initial (1). □

COROLLAIRE 2.6. *Si à l'une des équations du système d'équations linéaires on ajoute une combinaison linéaire d'autres équations du système, on aboutit à un système d'équations équipotent au système de départ.*

COROLLAIRE 2.7. *Si l'on élimine du système d'équations linéaires ou si l'on adjoint à ce système une équation constituant une combinaison linéaire d'autres équations du système, on obtient alors un système d'équations équipotent à celui de départ.*

Egalité de rangs des lignes et des colonnes de la matrice. Soit $\mathcal{F}$ un corps. Le tableau de la forme

$$(1)\quad A = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \ldots & \ldots & \ldots \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{bmatrix},$$

où $\alpha_{ik} \in F$, est appelé *matrice* associé au corps $\mathcal{F}$ ou matrice $m \times n$ sur $\mathcal{F}$. Introduisons les notations suivantes pour les lignes et les colonnes d'une matrice: la i-ème ligne de la matrice est notée A_i, $A_i = [\alpha_{i1}, \ldots, \alpha_{in}]$; la k-ième colonne de la matrice est notée A^k:

$$A^k = \begin{bmatrix} \alpha_{1k} \\ \cdot \\ \cdot \\ \cdot \\ \alpha_{mk} \end{bmatrix}.$$

Les lignes de la matrice A peuvent être assimilées à des vecteurs arithmétiques à n dimensions sur $\mathcal{F}$. Les colonnes de la matrice A peuvent être prises pour des vecteurs à m dimensions sur $\mathcal{F}$.

DÉFINITION. On appelle *rang de la ligne de la matrice A* le rang du système de ses lignes $A_1, \ldots, A_m$ assimilées à des vecteurs de

dimension n sur $\mathcal{F}$. On nomme *rang de la colonne de la matrice A* le rang du système de ses colonnes $A^1, \ldots, A^n$, prises pour des vecteurs de dimension m sur $\mathcal{F}$.

Le rang de la ligne de la matrice A est noté $r(A)$, celui de la colonne $\rho(A)$.

La matrice obtenue de la matrice A par substitution à ses lignes des colonnes correspondantes est dite *transposée* de A et notée ${}^tA$,

$$ {}^tA = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{m1} \\ \cdot & \cdot\cdot\cdot\cdot & \cdot \\ \alpha_{1n} & \ldots & \alpha_{mn} \end{bmatrix}. $$

Par les symboles $r({}^tA)$ et $\rho({}^tA)$ on désigne respectivement les rangs des lignes et des colonnes de la matrice ${}^tA$.

Soit

$$ (1) \qquad \begin{array}{l} \alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_{m1}x_1 + \ldots + \alpha_{mn}x_n = 0 \end{array} $$

un système homogène d'équations linéaires. La matrice A

$$ A = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \cdot & \cdot\cdot\cdot\cdot & \cdot \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{bmatrix} $$

est appelée *matrice* ou *matrice fondamentale* (ou de base) *du système d'équations* (1).

THÉORÈME 2.8. *Si un système homogène d'équations linéaires sur un corps* $\mathcal{F}$

$$ (1) \qquad \begin{array}{l} \alpha_{11}\lambda_1 + \ldots + \alpha_{1n}\lambda_n = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_{k1}\lambda_1 + \ldots + \alpha_{kn}\lambda_n = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_{m1}\lambda_1 + \ldots + \alpha_{mn}\lambda_n = 0 \end{array} $$

aux variables $\lambda_1, \ldots, \lambda_n$ *est équipotent au système*

$$ (2) \qquad \begin{array}{l} \alpha_{11}\lambda_1 + \ldots + \alpha_{1n}\lambda_n = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_{k1}\lambda_1 + \ldots + \alpha_{kn}\lambda_n = 0, \end{array} $$

composé des k premières équations du système (1), *les rangs des colonnes des matrices de ces systèmes sont alors égaux.*

D é m o n s t r a t i o n. Soient A et $\bar{A}$ les matrices des systèmes d'équations (1) et (2) respectivement. Si $\bar{A}$ est une matrice nulle, alors tout vecteur de F^n est une solution du système (2). En vertu de l'équipotence des systèmes (1) et (2), il s'ensuit que chaque vecteur de F^n est une solution du système (1). Donc, la matrice A est nulle et son rang est zéro.

Admettons maintenant que $\bar{A}$ est une matrice non nulle et que

$$(3)\quad \bar{A}^1, \ldots, \bar{A}^r$$

est une base du système des colonnes de la matrice $\bar{A}$. Alors en vertu de l'équipotence des systèmes (1) et (2) le système $A^1, \ldots, A^r$ des r premières colonnes de la matrice A est linéairement indépendant. Si $r < s \leqslant n$, le système des colonnes $A^1, \ldots, A^r, A^s$ est linéairement dépendant. Dans le cas contraire, en vertu de l'équipotence de (1) et (2) le système $\bar{A}^1, \ldots, \bar{A}^r, \bar{A}^s$ des colonnes de la matrice $\bar{A}$ serait linéairement indépendant, ce qui contredirait l'hypothèse (3). Le système $A^1, \ldots, A^r$ est donc la base du système des colonnes de la matrice A. Par conséquent, les rangs des colonnes des matrices A et $\bar{A}$ sont les mêmes. □

THÉORÈME 2.9. *Le rang de la ligne d'une matrice est égal au rang de sa colonne.*

D é m o n s t r a t i o n. Le théorème est apparemment vrai pour des matrices nulles. Supposons que $A = \| \alpha_{ik} \|$ est une matrice non nulle sur le corps $\mathcal{F}$ et que ses r premières lignes forment la base du système des lignes de cette matrice. Considérons un système homogène d'équations linéaires sur $\mathcal{F}$

$$(1)\quad \begin{array}{l} \alpha_{11}\lambda_1 + \ldots + \alpha_{1n}\lambda_n = 0, \\ \ldots\ldots\ldots\ldots\ldots \\ \alpha_{r1}\lambda_1 + \ldots + \alpha_{rn}\lambda_n = 0, \\ \ldots\ldots\ldots\ldots\ldots \\ \alpha_{m1}\lambda_1 + \ldots + \alpha_{mn}\lambda_n = 0 \end{array}$$

par rapport aux variables $\lambda_1, \ldots, \lambda_n$ pour lequel A est une matrice. Considérons également un système homogène

$$(2)\quad \begin{array}{l} \alpha_{11}\lambda_1 + \ldots + \alpha_{1n}\lambda_n = 0, \\ \ldots\ldots\ldots\ldots\ldots \\ \alpha_{r1}\lambda_1 + \ldots + \alpha_{rn}\lambda_n = 0, \end{array}$$

composé des r premières équations du système (1); désignons sa matrice par $\bar{A}$. Comme les r premières lignes de la matrice A constituent la base du système de ses lignes, chaque équation du système (1) est donc une combinaison linéaire des équations du systè-

me (2). Donc, les systèmes d'équations (1) et (2) sont équipotents. Selon le théorème 2.8 il s'ensuit de l'équipotence des systèmes (1) et (2) l'égalité des rangs des colonnes des matrices de ces systèmes, c'est-à-dire

(3) $\rho(A) = \rho(\bar{A})$.

Puisque les colonnes de la matrice $\bar{A}$ constituent des vecteurs de dimension r sur $\mathcal{F}$, selon le corollaire 1.6 $\rho(\bar{A}) \leqslant r = r(A)$. Donc, en vertu de (3), on a

(4) $\rho(A) \leqslant r(A)$.

Une inégalité analogue s'obtient également pour la matrice transposée ${}^tA$, c'est-à-dire qu'on a

(5) $\rho({}^tA) \leqslant r({}^tA)$.

On voit sans peine que $\rho({}^tA) = r(A)$, $r({}^tA) = \rho(A)$. D'où en vertu de (5), il vient

(6) $r(A) \leqslant \rho(A)$.

Sur la base de (4) et (6) on conclut que $r(A) = \rho(A)$. □

Critère de compatibilité du système d'équations linéaires. Considérons un système d'équations linéaires sur le corps $\mathcal{F}$:

(1) $\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = \beta_i \quad (i = 1, \ldots, m)$.

Les matrices

$$A = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \cdot & \cdot\cdot\cdot & \cdot \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{bmatrix} \quad \text{et} \quad B = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} & \beta_1 \\ \cdot & \cdot\cdot\cdot & \cdot & \cdot \\ \alpha_{m1} & \ldots & \alpha_{mn} & \beta_m \end{bmatrix}$$

sont appelées respectivement *matrices fondamentale* et *complète* du système d'équations (1). Le vecteur **b**

$$\mathbf{b} = \begin{bmatrix} \beta_1 \\ \cdot \\ \cdot \\ \cdot \\ \beta_m \end{bmatrix}$$

est nommé *colonne des termes libres*.

Considérons l'équation (sur le corps $\mathcal{F}$)

(2) $x_1A^1 + \ldots + x_nA^n = \mathbf{b}$,

où $A^1, \ldots, A^n$ est le vecteur colonne de la matrice A.

THÉORÈME 2.10. *L'équation* (2) *est équipotente au système d'équations* (1).

D é m o n s t r a t i o n. Soit $(\xi_1, \ldots, \xi_n)$ toute solution du système (1), c'est-à-dire

$$(3) \qquad \alpha_{i1}\xi_1 + \ldots + \alpha_{in}\xi_n = \beta_i \quad (i = 1, \ldots, m).$$

Compte tenu de

$$(4) \qquad \xi_1 A^1 + \ldots + \xi_n A^n = \begin{bmatrix} \alpha_{11}\xi_1 + \ldots + \alpha_{1n}\xi_n \\ \ldots\ldots\ldots\ldots \\ \alpha_{m1}\xi_1 + \ldots + \alpha_{mn}\xi_n \end{bmatrix},$$

les égalités (3) peuvent être écrites en une seule égalité

$$(2') \qquad \xi_1 A^1 + \ldots + \xi_n A^n = \mathbf{b}.$$

Et, réciproquement: supposons que le vecteur $(\xi_1, \ldots, \xi_n)$ est solution de l'équation (2), c'est-à-dire qu'on a l'égalité (2'). Alors, en vertu de (4), à partir de (2') s'ensuivent les égalités (3). Ainsi, toute solution de l'équation (2) est solution du système (1). Par conséquent, l'équation (2) est équipotente au système d'équations (1). □

COROLLAIRE 2.11. *Un système homogène d'équations linéaires*

$$\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \qquad (i = 1, \ldots, m)$$

est équipotent à l'équation

$$x_1 A^1 + \ldots + x_n A^n = \mathbf{0},$$

où $\mathbf{0}$ *est le vecteur colonne nul à* m *dimensions.*

L'équation (2) est appelée *forme vectorielle de notation du système d'équations linéaires* (1).

THÉORÈME 2.12. *Soient A et B respectivement les matrices fondamentale et complète du système d'équations linéaires* (1). *Les affirmations suivantes sont équipotentes*:

I. *Le système d'équations linéaires* (1) *est compatible.*

II. *L'équation* (2) *admet une solution (sur le corps* $\mathcal{F}$*).*

III. *Le vecteur* $\mathbf{b}$ *est une combinaison linéaire des colonnes de la matrice* A, c'est-à-dire $\mathbf{b} \in L(A^1, \ldots, A^n)$.

IV. *Les rangs des colonnes (des lignes) des matrices A et B sont égaux,* $r(A) = r(B)$.

D é m o n s t r a t i o n. En vertu de théorème 2.10 l'affirmation I entraîne l'affirmation II.

Si l'équation (2) a une solution, le vecteur $\mathbf{b}$ peut alors être représenté sous forme d'une combinaison linéaire (avec coefficients du corps $\mathcal{F}$) des colonnes de la matrice A. Par conséquent, III s'ensuit de II.

Si $\mathbf{b} \in L(A^1, \ldots, A^n)$, le système des colonnes $A^1, \ldots, A^n$ de la matrice A est équivalent au système des colonnes $A^1, \ldots, A^n$, b de la matrice B. Selon la proposition 1.12 cela entraîne l'égalité

des rangs des colonnes des matrices A et B. Donc, l'affirmation III implique IV.

Supposons que les rangs des colonnes des matrices A et B sont les mêmes. Dans ce cas la base du système des colonnes de la matrice A est aussi une base du système des colonnes de la matrice B. Par conséquent, $\mathbf{b} \in L(A^1, \ldots, A^n)$, c'est-à-dire qu'il existe des scalaires $\lambda_1, \ldots, \lambda_n \in F$ tels que $\lambda_1 A^1 + \ldots + \lambda_n A^n = \mathbf{b}$. Cette dernière égalité traduit que le vecteur $(\lambda_1, \ldots, \lambda_n)$ est solution de l'équation (2) et, en vertu du théorème 2.10, solution du système d'équations (1). Ainsi, de l'assertion IV s'ensuit l'assertion I. Par conséquent, les assertions I, II, III et IV sont équipotentes. □

THÉORÈME 2.13 (de KRONECKER-CAPELLI). *Un système d'équations linéaires est compatible si et seulement si le rang de la matrice fondamentale est égal à celui de la matrice complète.*

Ce théorème découle directement du théorème précédent.

COROLLAIRE 2.14. *Si le rang de la matrice d'un système d'équations linéaires est égal au nombre d'équations du système, ce système d'équations est compatible.*

D é m o n s t r a t i o n. Soient A et B respectivement les matrices fondamentale et complète du système de m équations linéaires à n variables. On a alors $\rho(B) \geqslant \rho(A) = m$. D'autre part, $\rho(B) \leqslant m$, car la matrice B possède m lignes. Par suite, $\rho(B) = \rho(A)$. Donc, selon le théorème 2.13, le système considéré d'équations linéaires est compatible. □

Connexion entre les solutions d'un système linéaire inhomogène et les solutions d'un système homogène qui lui est associé. Soit donné un système linéaire inhomogène

$$(1) \quad \alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = \beta_i \quad (i = 1, \ldots, m)$$

sur le corps $\mathcal{F}$. Le système d'équations linéaires

$$(2) \quad \alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \quad (i = 1, \ldots, m)$$

est dit *système homogène* associé au système (1).

Soient L l'ensemble de toutes les solutions du système homogène (2) et $\mathbf{c}$ une solution quelconque du système (1). L'ensemble $\{\mathbf{c} + \mathbf{d} \mid \mathbf{d} \in L\}$ sera noté $\mathbf{c} + L$:

$$\mathbf{c} + L = \{\mathbf{c} + \mathbf{d} \mid \mathbf{d} \in L\}.$$

PROPOSITION 2.15. *Si la solution du système inhomogène* (1) *est additionnée à la solution du système homogène* (2), *on obtient la solution du système* (1).

D é m o n s t r a t i o n. Soient $(\gamma_1, \ldots, \gamma_n)$ la solution du système (1) et $(\delta_1, \ldots, \delta_n)$ la solution du système (2), autrement dit,

$$\alpha_{i1}\gamma_1 + \ldots + \alpha_{in}\gamma_n = \beta_i \quad (i = 1, \ldots, m),$$
$$\alpha_{i1}\delta_1 + \ldots + \alpha_{in}\delta_n = 0 \quad (i = 1, \ldots, m).$$

En additionnant terme à terme ces égalités on obtient les égalités

$$\alpha_{i1}(\gamma_1 + \delta_1) + \ldots + \alpha_{in}(\gamma_n + \delta_n) = \beta_i \quad (i = 1, \ldots, m),$$

qui montrent que le vecteur $(\gamma_1 + \delta_1, \ldots, \gamma_n + \delta_n)$ est une solution du système (1). □

PROPOSITION 2.16. *La différence entre deux solutions quelconques du système inhomogène d'équations linéaires est une solution du système homogène associé à lui.*

Démonstration. Soient $(\gamma_1, \ldots, \gamma_n)$ et $(\gamma'_1, \ldots, \gamma'_n)$ des solutions du système inhomogène d'équations (1), autrement dit,

$$\alpha_{i1}\gamma_1 + \ldots + \alpha_{in}\gamma_n = \beta_i \quad (i = 1, \ldots, m),$$
$$\alpha_{i1}\gamma'_1 + \ldots + \alpha_{in}\gamma'_n = \beta_i \quad (i = 1, \ldots, m).$$

En soustrayant terme à terme, on aboutit aux égalités

$$\alpha_{i1}(\gamma_1 - \gamma'_1) + \ldots + \alpha_{in}(\gamma_n - \gamma'_n) = 0 \quad (i = 1, \ldots, m),$$

qui montrent que le vecteur $(\gamma_1 - \gamma'_1, \ldots, \gamma_n - \gamma'_n)$ est *solution du système homogène d'équations* (2). □

THÉORÈME 2.17. *Soient* $\mathbf{c}$ *la solution du système inhomogène d'équations linéaires* (1) *et* L *l'ensemble de toutes les solutions du système homogène* (2) *associé au système* (1). *Dans ce cas* $\mathbf{c} + L$ *est l'ensemble de toutes les solutions du système* (1).

Démonstration. Soient M l'ensemble de toutes les solutions du système (1) et $\mathbf{c} \in M$. Chaque élément de l'ensemble $\mathbf{c} + L$ peut se représenter en forme de somme $\mathbf{c} + \mathbf{l}$, où $\mathbf{l} \in L$. En vertu de la proposition 2.15, $\mathbf{c} + \mathbf{l} \in M$. Donc,

(3) $\quad \mathbf{c} + L \subset M.$

L'inclusion inverse est également vraie. En effet, si $\mathbf{d}$ est une solution quelconque du système (1), $\mathbf{c} \in M$, alors, en vertu de la proposition 2.16, $\mathbf{d} - \mathbf{c} \in L$. Donc, on a $\mathbf{d} \in \mathbf{c} + L$; par conséquent,

(4) $\quad M \subset \mathbf{c} + L.$

Sur la base de (3) et (4) on conclut que $M = \mathbf{c} + L$. □

COROLLAIRE 2.18. *Un système d'équations linéaires inhomogène compatible admet une solution unique si et seulement si le système d'équations homogène qui lui est associé a une solution unique (nulle).*

COROLLAIRE 2.19. *Si deux systèmes inhomogènes d'équations linéaires (sur le corps* $\mathcal{F}$*) à n variables* $x_1, \ldots, x_n$ *sont compatibles et équipotents, les systèmes homogènes d'équations qui leur sont associés sont également équipotents.*

Théorèmes impliqués par un système d'équations linéaires. Considérons le système d'équations linéaires

(I) $\quad \alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = \beta_i \qquad (i = 1, \ldots, m)$

sur le corps $\mathscr{F}$. L'équation linéaire

(II) $\gamma_1 x_1 + \ldots + \gamma_n x_n = \beta$,

où $\gamma_1, \ldots, \gamma_n \in F$ est appelée *implication du système* (I) si chaque solution du système (I) est solution de cette équation.

Selon la proposition 2.1, toute combinaison linéaire (à coefficients du corps $\mathscr{F}$) d'équations du système (I) est une implication de ce système. Est-ce que la réciproque est vraie? La réponse à cette question nous est fournie par les théorèmes suivants.

THÉORÈME 2.20. *L'équation linéaire*

(2) $\gamma_1 x_1 + \ldots + \gamma_n x_n = 0$,

qui est une implication du système homogène d'équations

(1) $\alpha_{i1} x_1 + \ldots + \alpha_{in} x_n = 0 \quad (i = 1, \ldots, m)$,

constitue une combinaison linéaire d'équations de ce système.

Démonstration. Par hypothèse, l'équation (2) est l'implication du système (1). Donc, le système

$$(3) \quad \begin{aligned} &\alpha_{11} x_1 + \ldots + \alpha_{1n} x_n = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &\alpha_{m1} x_1 + \ldots + \alpha_{mn} x_n = 0, \\ &\gamma_1 x_1 + \ldots + \gamma_n x_n = 0 \end{aligned}$$

est équipotent au système (1). Selon les théorèmes 2.8 et 2.9 il s'ensuit que le rang de la matrice A du système (1) est égal à celui de la matrice $\bar{A}$ du système (3). Aussi si $\mathbf{c} = (\gamma_1, \ldots, \gamma_n)$, a-t-on

$$\text{rang}\,\{A_1, \ldots, A_m, \mathbf{c}\} = \text{rang}\,\{A_1, \ldots, A_m\},$$

où A_i est la i-ième ligne de la matrice A. Sur la base de cette égalité on conclut que $\mathbf{c}$ est une combinaison linéaire des lignes $A_1, \ldots, A_m$ de la matrice A. Par conséquent, l'équation (2) est une combinaison linéaire d'équations du système (1). □

THÉORÈME 2.21. *Deux systèmes homogènes d'équations linéaires sur le corps $\mathscr{F}$ à n variables $x_1, \ldots, x_n$ sont équipotents si et seulement si les matrices de ces systèmes sont équivalentes par lignes.*

Ce théorème se déduit facilement du théorème 2.20.

THÉORÈME 2.22. *Une équation linéaire constituant une implication d'un système compatible d'équations linéaires est une combinaison linéaire d'équations de ce système.*

Démonstration. Admettons que l'équation (II) est une implication du système compatible (I). Dans ce cas, le système d'équations

$$(3) \quad \begin{aligned} &\alpha_{11} x_1 + \ldots + \alpha_{1n} x_n = \beta_1, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &\alpha_{m1} x_1 + \ldots + \alpha_{mn} x_n = \beta_m, \\ &\gamma_1 x_1 + \ldots + \gamma_n x_n = \beta \end{aligned}$$

est compatible et équipotent au système (I). Selon le corollaire 2.19 il s'ensuit une équipotence de systèmes homogènes appropriés, c'est-à-dire que le système d'équations

$$(4) \qquad \alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \qquad (i = 1, \ldots, m)$$

est équipotent au système d'équations

$$(5) \qquad \begin{aligned} &\alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &\alpha_{m1}x_1 + \ldots + \alpha_{mn}x_n = 0, \\ &\gamma_1 x_1 + \ldots + \gamma_n x_n = 0. \end{aligned}$$

En vertu des théorèmes 2.8 et 2.9 le rang de la matrice A du système (4) est égal au rang de la matrice $\bar{A}$ du système (5). Donc, les rangs des matrices fondamentales des systèmes (1) et (3) sont égaux. Comme les systèmes (1) et (3) sont compatibles, selon le critère de compatibilité, il s'ensuit que le rang des lignes de la matrice complète B du système (1) est égal au rang des lignes de la matrice complète $\bar{B}$ du système (3). En s'appuyant sur l égalité de ces rangs on conclut que la dernière ligne de la matrice $\bar{B}$ est une combinaison linéaire des lignes de la matrice B, c'est-à-dire que

$$(\gamma_1, \ldots, \gamma_n, \beta) \in L(B_1, \ldots, B_n).$$

Par conséquent, l'équation (II) est une combinaison linéaire d'équations du système (I). □

Exercices

1. Soit A une matrice $n \times m$ à lignes linéairement indépendantes. Démontrer que $m \geqslant n$.

2. Démontrer que le rang r d'une matrice $m \times n$ n'est pas supérieur à m et n, $r \leqslant \min(m, n)$.

3. Démontrer qu'en éliminant une ligne (une colonne) dans une matrice, on ne modifie pas son rang si et seulement si la ligne (la colonne) éliminée s'exprime linéairement en fonction des autres lignes (colonnes).

4. Démontrer que l'adjonction à une matrice d'une ligne (d'une colonne) ou bien ne modifie pas son rang ou bien l'augmente d'une unité.

5. Démontrer que si le rang de la matrice A ne varie pas après adjonction à cette dernière d'une colonne quelconque de la matrice B au même nombre de lignes, ce rang ne varie de même pas après adjonction à la matrice A de toutes les colonnes de la matrice B.

6. Supposons que la matrice B s'obtient à partir de la matrice A par une série de transformations linéaires régulières des lignes. Démontrer que les lignes de la matrice A sont linéairement indépendantes si et seulement si les lignes de la matrice B sont linéairement indépendantes.

7. Soient A et B des matrices à n colonnes. Démontrer que les matrices A et B sont équivalentes par lignes au cas où l'enveloppe linéaire des lignes de la matrice A coïncide avec l'enveloppe linéaire des lignes de la matrice B.

8. Soient A une matrice $m \times n$ et B une matrice $m \times (n+k)$ obtenue à partir de la matrice A par adjonction de k colonnes nouvelles. Démontrer que

(a) si les lignes de la matrice B sont linéairement dépendantes, les lignes de la matrice A le sont aussi;

(b) si les lignes de la matrice A sont linéairement indépendantes, les lignes de la matrice B le sont aussi;

(c) le rang de la matrice A n'est pas supérieur à celui de la matrice B.

9. Le rang de la matrice d'un système homogène d'équations linéaires est inférieur d'une unité au nombre de variables. Démontrer que toutes deux solutions de ce système sont proportionnelles (c'est-à-dire qu'elles ne diffèrent que d'un facteur scalaire).

10. Chercher les conditions pour lesquelles avec toute solution d'un système homogène d'équations linéaires la k-ième variable est nulle.

11. Démontrer que si un système d'équations linéaires sur le corps $\mathfrak{A}$ des nombres rationnels n'a pas de solutions dans $\mathfrak{A}$, il ne possède pas de solutions dans tout corps numérique.

12. Soit donné le système homogène d'équations linéaires (1) (sur le corps $\mathfrak{A}$ des nombres rationnels) possédant des solutions non nulles. Tout système fondamental des solutions du système (1) sur $\mathfrak{A}$ est un système fondamental sur tout corps numérique.

13. Soit

$$(1) \qquad \alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \qquad (i = 1, \ldots, m)$$

un système homogène d'équations linéaires (sur le corps $\mathcal{F}$). Démontrer que l'équation

$$\beta_1x_1 + \ldots + \beta_nx_n = 0$$

est une implication du système (1) si et seulement si elle est une combinaison linéaire des équations (1).

§ 3. Matrices en escalier et systèmes d'équations linéaires

Matrices en escalier. Soit

$$A = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \cdot & \cdot\cdot\cdot\cdot & \cdot \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{bmatrix}$$

la matrice $m \times n$ sur le corps $\mathcal{F}$. L'*élément pivot de la ligne de la matrice* est son premier élément (en comptant à partir de la gauche) non nul. La colonne de la matrice est dite *fondamentale* si elle contient l'élément pivot d'une ligne quelconque de la matrice.

DÉFINITION. La matrice A est dite *en escalier* si elle satisfait aux conditions:

(1) les lignes à éléments nuls (si elles existent) se disposent au-dessous de toutes les lignes à éléments non nuls;

(2) si $\alpha_{1k_1}, \alpha_{2k_2}, \ldots, \alpha_{rk_r}$ sont des éléments pivots des lignes à éléments non nuls de la matrice, alors $k_1 < k_2 < \ldots < k_r$.

Exemples de matrices en escalier: 1) la matrice nulle, 2) la matrice uniligne, 3) la matrice unité, 4) la matrice triangulaire

supérieure

$$\begin{bmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ 0 & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_{nn} \end{bmatrix}.$$

Au système des vecteurs lignes (colonnes) de cette matrice on peut appliquer les transformations élémentaires.

DÉFINITION. Les transformations élémentaires sur un système de lignes (de colonnes) d'une matrice sont appelées *transformations élémentaires de la matrice*. Deux matrices sont dites *équivalentes par lignes* si l'une est obtenue à partir de l'autre par une série de transformations élémentaires sur les lignes.

La relation d'équivalence par lignes est réflexive, symétrique et transitive, c'est-à-dire est une relation d'équivalence.

DÉFINITION. On appelle *rang de ligne de la matrice* le rang du système de ses lignes. On appelle *rang de colonne de la matrice* le rang du système de ses colonnes.

De cette définition, en vertu du théorème 1.8, s'ensuit la proposition 3.1.

PROPOSITION 3.1. *Si une matrice s'obtient de l'autre à la suite d'une série de transformations élémentaires sur des lignes, les rangs de ligne de ces matrices sont alors égaux.*

THÉORÈME 3.2. *Toute matrice $m \times n$ est équivalente par lignes à une matrice $m \times n$ en escalier.*

D é m o n s t r a t i o n (par récurrence sur le nombre de lignes de la matrice). Si le nombre de lignes de la matrice est égal à l'unité, la matrice est alors en escalier. En posant que le théorème est vrai pour des matrices à $m - 1$ lignes, démontrons qu'il est aussi vrai pour des matrices à m lignes. Soit A une matrice à m lignes:

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{bmatrix}.$$

Si dans la première colonne de la matrice on a un élément différent de zéro, on peut permuter cette ligne à élément non nul avec la première ligne. On montre sans peine qu'une permutation de lignes est l'aboutissement d'une série de transformations élémentaires sur des lignes. Aussi admettra-t-on que $\alpha_{11} \neq 0$. La matrice A peut être transformée en la matrice B:

$$B = \begin{bmatrix} 1 & \beta_{12} & \dots & \beta_{1n} \\ 0 & \beta_{22} & \dots & \beta_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & \beta_{m2} & \dots & \beta_{mn} \end{bmatrix}$$

par une série de transformations élémentaires. A cette fin la première ligne de la matrice A doit être multipliée par α_{11}^{-1}. Ensuite, la première ligne obtenue, multipliée par $(-\alpha_{ik})$, est ajoutée à la i-ième ligne pour $i = 2, \ldots, m$. La matrice formée à partir de B par élimination de la première ligne comporte $m - 1$ lignes et, par hypothèse de récurrence, est équivalente par lignes à une certaine matrice $(m - 1) \times n$ en escalier C^*:

$$\begin{bmatrix} 0 & \beta_{22} & \ldots & \beta_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & \beta_{m2} & \ldots & \beta_{mn} \end{bmatrix} \sim C^* = \begin{bmatrix} 0 & \gamma_{22} & \ldots & \gamma_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & \gamma_{m2} & \ldots & \gamma_{mn} \end{bmatrix}.$$

En s'appuyant sur ce fait ainsi que sur l'équivalence par lignes des matrices A et B, on peut conclure que la matrice A est équivalente par lignes à la matrice en escalier C:

$$C = \begin{bmatrix} 1 & \beta_{12} & \ldots & \beta_{1n} \\ 0 & \gamma_{22} & \ldots & \gamma_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & \gamma_{m2} & \ldots & \gamma_{mn} \end{bmatrix}.$$

La matrice C est en escalier vu que la matrice C^* l'est aussi.

Si la première colonne ou plusieurs premières colonnes de la matrice A ont partout des zéros, on considérera la matrice obtenue par élimination de ces colonnes. Cette matrice comporte dans la première colonne un élément non nul. Il s'ensuit donc de la première partie de la démonstration que cette matrice est équivalente par lignes à une matrice en escalier. On constate aussitôt qu'en adjoignant à gauche à cette matrice en escalier les colonnes à éléments partout nuls éliminées précédemment, on aboutit à une matrice équivalente par lignes à la matrice de départ A. □

THÉORÈME 3.3. *Le rang des lignes d'une matrice en escalier est égal au nombre de ses lignes à éléments non nuls.*

D é m o n s t r a t i o n. Le théorème est apparemment vrai pour une matrice nulle. Supposons que A est une matrice en escalier de r lignes à éléments non nuls. Par commodité d'écriture posons que les éléments pivots de la matrice A occupent les r premières colonnes, autrement dit,

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1r} & \ldots \\ 0 & \alpha_{22} & \ldots & \alpha_{2r} & \ldots \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & \alpha_{rr} & \ldots \\ 0 & 0 & \ldots & 0 & \ldots \end{bmatrix},$$

où $\alpha_{ii} \neq 0$ pour $i = 1, \ldots, r$. Ainsi, les r premières lignes $A_1, \ldots$ $\ldots, A_r$ de la matrice A n'ont pas partout des zéros, tandis que

les autres (si elles existent) ont partout des zéros. Montrons que les lignes $A_1, \ldots, A_r$ sont linéairement indépendantes. Il faut montrer que pour tous scalaires $\lambda_1, \ldots, \lambda_r$ de l'égalité

(1) $\lambda_1 A_1 + \ldots + \lambda_r A_r = 0$

s'ensuivent les égalités

(2) $\lambda_1 = 0, \ldots, \lambda_r = 0.$

Vu que

$$\lambda_1 A_1 + \ldots + \lambda_r A_r =$$
$$= (\lambda_1 \alpha_{11}, \lambda_1 \alpha_{12} + \lambda_2 \alpha_{22}, \ldots, \lambda_1 \alpha_{1r} + \ldots + \lambda_r \alpha_{rr}, \ldots),$$

de (1) s'ensuivent les égalités

$$(3) \quad \begin{aligned} &\lambda_1 \alpha_{11} = 0, \\ &\lambda_1 \alpha_{12} + \lambda_2 \alpha_{22} = 0, \\ &\ldots\ldots\ldots\ldots\ldots \\ &\lambda_1 \alpha_{1r} + \ldots + \lambda_r \alpha_{rr} = 0. \end{aligned}$$

Puisque $\alpha_{ii} \neq 0$ pour $i = 1, \ldots, r$ de (3) s'ensuivent les égalités (2). Ainsi, le système $A_1, \ldots, A_r$ de lignes à éléments partout non nuls de la matrice A est linéairement indépendant. Par conséquent, le rang de ligne de la matrice A vaut r. Dans le cas général la démonstration est effectuée de façon analogue. □

En s'appuyant sur le théorème 3.3 on aboutit à la règle de calcul suivante du rang de la matrice. *Pour calculer le rang de ligne de la matrice A il faut la réduire à la forme en escalier C par une série de transformations élémentaires sur les lignes. Le nombre des lignes à éléments non nuls de la matrice C est égal au rang des lignes de la matrice A.*

Matrices en escalier réduites. Lors de la résolution et de l'étude d'un système d'équations linéaires un rôle important revient aux matrices en escalier réduites.

DÉFINITION. Une matrice en escalier est dite *réduite* si la matrice composée de toutes ses colonnes fondamentales est une matrice unité.

Une matrice en escalier réduite ne possède pas de lignes à éléments partout nuls et tous les éléments pivots de ses lignes sont égaux à l'unité.

THÉORÈME 3.4. *Toute matrice non nulle est équivalente par lignes à la matrice en escalier réduite.*

D é m o n s t r a t i o n. Soit A une matrice non nulle de rang r. Selon les théorèmes 3.2 et 3.3 elle est équivalente par lignes à la matrice en escalier, par exemple, à la matrice B composée de r lignes à éléments non nuls. Divisons chaque ligne de la matrice B

par son élément pivot. On aboutit à une matrice C en escalier dont tous les éléments pivots des lignes sont égaux à l'unité. Ensuite, par une série de transformations élémentaires des lignes de la matrice C on égale à zéro tous les éléments non nuls se disposant au-dessus des éléments pivots. On obtient une matrice D dont les colonnes fondamentales constituent la matrice unité. Par conséquent, D est la matrice en escalier réduite cherchée qui est équivalente par lignes à la matrice initiale A. □

THÉORÈME 3.5. *Toute matrice carrée $n \times n$ à lignes linéairement indépendantes est équivalente par lignes à la matrice unité $n \times n$ E.*

Démonstration. Soit A la matrice $n \times n$ à lignes linéairement indépendantes. Au moyen d'une série de transformations élémentaires régulières des lignes elle peut être réduite à une matrice $n \times n$ en escalier $C = \| \gamma_{ik} \|$. Soient $\gamma_{1k_1}, \gamma_{2k_2}, \ldots, \gamma_{nk_n}$ les éléments pivots de la matrice C. On a alors

(1) $\gamma_{1k_1} \neq 0, \ldots, \gamma_{nk_n} \neq 0,$

(2) $1 \leqslant k_1 < k_2 < \ldots < k_n \leqslant n.$

Des inégalités (2) il s'ensuit que $k_1 = 1$, $k_2 = 2, \ldots, k_n = n$. La matrice C est donc de l'aspect

$$C = \begin{bmatrix} \gamma_{11} & \gamma_{12} & \ldots & \gamma_{1n} \\ 0 & \gamma_{22} & \ldots & \gamma_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \gamma_{nn} \end{bmatrix},$$

autrement dit, est une matrice triangulaire supérieure à éléments non nuls sur la diagonale principale. Multiplions la première ligne de la matrice par γ_{11}^{-1}, la seconde par γ_{22}^{-1}, etc. On aboutit ainsi à une matrice équivalente par lignes

$$C' = \begin{bmatrix} 1 & \gamma'_{12} & \ldots & \gamma'_{1n} \\ 0 & 1 & \ldots & \gamma'_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 \end{bmatrix}.$$

On constate sans peine que la matrice C' est équivalente par lignes à la matrice unité $n \times n$ E. Il existe donc une série de transformations élémentaires (régulières) des lignes qui réduit la matrice A en une matrice unité E. □

Systèmes homogènes d'équations linéaires. Considérons un système homogène d'équations sur le corps $\mathscr{F}$

$$(1) \quad \begin{aligned} \alpha_{11}x_1 + \ldots + \alpha_{1n}x_n &= 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_{m1}x_1 + \ldots + \alpha_{mn}x_n &= 0. \end{aligned}$$

Soit

$$A = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \dots & \dots & \dots \\ \alpha_{m1} & \dots & \alpha_{mn} \end{bmatrix}$$

une matrice composée des coefficients attachés aux variables et appelée *matrice fondamentale du système* (1), $A^1, \dots, A^n$ étant les colonnes de cette matrice. L'équation (sur $\mathcal{F}$)

$$(2) \qquad x_1A^1 + \dots + x_nA^n = 0,$$

où 0 est le vecteur colonne nul, est nommée *forme vectorielle d'écriture du système d'équations* (1).

Selon le corollaire 2.11 un système homogène d'équations (1) est équipotent à l'équation (2).

PROPOSITION 3.6. *Si la matrice A d'un système homogène d'équations* (1) *possède le rang $r > 0$ et $A_1, \dots, A_r$ est la base du système de ses lignes, le système* (1) *est alors équipotent au système*

$$(3) \qquad \begin{aligned} &\alpha_{11}x_1 + \dots + \alpha_{1n}x_n = 0, \\ &\dots\dots\dots\dots\dots\dots \\ &\alpha_{r1}x_1 + \dots + \alpha_{rn}x_n = 0, \end{aligned}$$

composé de r premières équations du système (1).

Démonstration. Vu que les r premières lignes de la matrice A constituent la base du système des lignes de cette matrice, chaque équation du système (1) est donc une combinaison linéaire des équations (3). De plus, le système (3) est une implication du système (1). Par conséquent, les systèmes (1) et (3) sont équipotents. □

PROPOSITION 3.7. *Un système homogène d'équations linéaires de matrice A possède des solutions non nulles si et seulement si les colonnes de la matrice A sont linéairement dépendantes.*

Cette proposition découle directement du corollaire 2.11.

COROLLAIRE 3.8. *Un système homogène d'équations linéaires à n variables possède des solutions non nulles si et seulement si le rang de la matrice du système est inférieur à n.*

COROLLAIRE 3.9. *Si le nombre d'équations d'un système homogène d'équations linéaires est inférieur au nombre des variables, le système a des solutions non nulles.*

PROPOSITION 3.10. *L'ensemble de toutes les solutions d'un système homogène d'équations linéaires est clos par rapport à l'addition, à la soustraction et à la multiplication par des scalaires. Toute combinaison linéaire de solutions d'un système homogène d'équations est une solution de ce système.*

La démonstration de la proposition 3.10 est laissée au soin du lecteur.

Système fondamental de solutions. Soit

$$(1)\quad \alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \qquad (i = 1, \ldots, m)$$

un système homogène d'équations linéaires sur le corps $\mathcal{F}$.

DÉFINITION. On appelle *système fondamental de solutions du système d'équations* (1) le système non vide linéairement indépendant de ses solutions dont l'enveloppe linéaire coïncide avec l'ensemble de toutes les solutions du système (1).

Notons que le système homogène d'équations linéaires ne possédant qu'une solution nulle n'a pas de système fondamental de solutions.

PROPOSITION 3.11. *Deux systèmes fondamentaux quelconques de solutions du système homogène d'équations linéaires admettent un même nombre de solutions.*

Démonstration. En effet, deux systèmes fondamentaux quelconques de solutions du système homogène d'équations (1) sont équivalents et linéairement indépendants. Aussi, en vertu de la proposition 1.12, leurs rangs sont-ils égaux. Donc, le nombre de solutions entrant dans l'un des systèmes fondamentaux est égal au nombre de solutions composant l'autre système fondamental de solutions. □

Si la matrice A d'un système homogène d'équations (1) est nulle, alors tout vecteur de F^n est solution du système (1); dans ce cas toute collection de n vecteurs linéairement indépendants de F^n est un système fondamental de solutions. Mais si le rang de la colonne de la matrice A est n, le système (1) n'admet alors qu'une solution, la solution nulle; donc, dans ce cas le système d'équations (1) est démuni de système fondamental de solutions.

THÉORÈME 3.12. *Si le rang r de la matrice d'un système homogène d'équations linéaires* (1) *est inférieur au nombre des variables n, le système* (1) *a alors un système fondamental de solutions comportant $n - r$ solutions.*

Démonstration. Si le rang de la matrice fondamentale A du système homogène (1) est égal à zéro ou à n, alors le théorème est vrai, comme il a été montré plus haut. C'est pourquoi on admet plus bas que $0 < r(A) < n$. En posant $r = r(A)$, on supposera que les r premières colonnes de la matrice A sont linéairement indépendantes. Dans ce cas la matrice A est équivalente par lignes à la matrice en escalier réduite, tandis que le système (1) est équivalent au système d'équations en escalier réduit suivant:

$$(2)\quad \begin{aligned} x_1 - \ldots - \gamma_{11}x_{r+1} - \ldots - \gamma_{1,n-r}x_n &= 0,\\ x_2 - \ldots - \gamma_{21}x_{r+1} - \ldots - \gamma_{2,n-r}x_n &= 0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots&\\ x_r - \gamma_{r1}x_{r+1} - \ldots - \gamma_{r,n-r}x_n &= 0. \end{aligned}$$

On vérifie sans peine qu'à tout système des valeurs de variables libres $x_{r+1}, \ldots, x_n$ du système (2) ne correspond qu'une et seulement une solution du système (2) et, partant, du système (1). En particulier, au système des valeurs nulles $x_{r+1} = 0, \ldots, x_n = 0$ ne correspond que la solution nulle du système (2) et du système (1).

Donnons dans le système (2) à l'une des variables libres la valeur égale à 1, tandis que les variables restantes seront considérées comme nulles. On obtient ainsi $n - r$ solutions du système d'équations (2) qu'on écrira sous forme de lignes de la matrice C:

$$C = \begin{bmatrix} \gamma_{11} & \gamma_{21} & \ldots & \gamma_{r1} & 1 & 0 & \ldots & 0 \\ \gamma_{12} & \gamma_{22} & \ldots & \gamma_{r2} & 0 & 1 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \gamma_{1n-r} & \gamma_{2n-r} & \ldots & \gamma_{r,\,n-r} & 0 & 0 & \ldots & 1 \end{bmatrix}.$$

Le système des lignes $C_1, \ldots, C_{n-r}$ de cette matrice est linéairement indépendant. En effet, pour tous scalaires $\lambda_1, \ldots, \lambda_{n-r}$ de l'égalité

$$\lambda_1 C_1 + \ldots + \lambda_{n-r} C_{n-r} = (0, 0, \ldots, 0)$$

s'ensuit l'égalité

$$(\ldots, \lambda_1, \lambda_2, \ldots, \lambda_{n-r}) = (0, 0, \ldots, 0)$$

et, partant, les égalités

$$\lambda_1 = 0, \lambda_2 = 0, \ldots, \lambda_{n-r} = 0.$$

Démontrons que l'enveloppe linéaire du système de lignes de la matrice C coïncide avec l'ensemble de toutes les solutions du système (1). Soit

$$\mathbf{a} = (\alpha_1, \ldots, \alpha_r, \alpha_{r+1}, \ldots, \alpha_n)$$

une solution quelconque du système (1). Le vecteur

$$\mathbf{d} = \mathbf{a} - (\alpha_{r+1} C_1 + \alpha_{r+2} C_2 + \ldots + \alpha_n C_{n-r})$$

est alors aussi une solution du système (1), de plus,

$$\mathbf{d} = (\delta_1, \ldots, \delta_r, 0, 0, \ldots, 0);$$

cette solution correspond aux valeurs nulles des variables libres $x_{r+1}, \ldots, x_n$. Aussi, $\mathbf{d}$ est-il une solution nulle du système (2) et du système (1); par conséquent,

$$\mathbf{a} = \alpha_{r+1} C_1 + \ldots + \alpha_n C_{n-r} \in L(C_1, \ldots, C_{n-r}).$$

Bref, on a démontré que l'ensemble de toutes les solutions du système (1) coïncide avec l'enveloppe linéaire du système des vecteurs $C_1, \ldots, C_{n-r}$. Donc, ce système de $n - r$ vecteurs est le système fondamental de solutions pour le système d'équations (1). □

COROLLAIRE 3.13. *Soient* **d** *une solution du système non homogène d'équations linéaires (sur le corps* $\mathscr{F}$*)*

$$\text{(I)} \qquad \alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = \beta_i \qquad (i = 1, \ldots, m)$$

et $C_1, \ldots, C_{n-r}$ *le système fondamental de solutions du système homogène d'équations*

$$\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n = 0 \qquad (i = 1, \ldots, m).$$

L'ensemble

$$\{\mathbf{d} + \lambda_1 C_1 + \ldots + \lambda_{n-r} C_{n-r} \mid \lambda_1, \lambda_2, \ldots, \lambda_{n-r} \in F\}$$

est alors l'ensemble de toutes les solutions du système (I).

Résolution du système d'équations linéaires par la méthode d'élimination successive des variables. Soit donné le système d'équations linéaires (sur le corps $\mathscr{F}$)

$$\text{(1)} \qquad \begin{aligned} &\alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = \beta_1, \\ &\ldots\ldots\ldots\ldots\ldots \\ &\alpha_{m1}x_1 + \ldots + \alpha_{mn}x_n = \beta_m. \end{aligned}$$

Posons

$$A = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \ldots & \ldots & \ldots \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{bmatrix}, \qquad B = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} & \beta_1 \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{m1} & \ldots & \alpha_{mn} & \beta_m \end{bmatrix}.$$

La matrice A est dite *matrice fondamentale du système* (1), la matrice B *matrice complète du système* (1).

Un système d'équations linéaires est dit *en escalier* si la matrice complète du système est une matrice en escalier sans lignes à éléments partout nuls. Un système d'équations linéaires est dit *système en escalier réduit* si la matrice complète du système est une matrice en escalier réduite.

Si B est une matrice nulle, alors tout vecteur à n dimensions de F^n est une solution du système (1). Mais si A est une matrice nulle, tandis que B ne l'est pas, le système d'équations (1) est alors incompatible.

Supposons que la matrice A n'est pas nulle. On peut alors réduire le système d'équations (1) à un système en escalier par des transformations élémentaires, et, ensuite, à un système en escalier réduit, ces systèmes étant équipotents au système initial (1). Supposons que les colonnes $A^1, \ldots, A^r$ constituent la base du système des colonnes de la matrice A. Au moyen d'une série de transformations élémentaires réduisons le système d'équations (1) à un système en escalier sans lignes à éléments partout nuls. Si cette dernière équation du système en escalier obtenu est de la forme

$$0 \cdot x_1 + \ldots + 0 \cdot x_n = \beta, \text{ où } \beta \neq 0,$$

le système d'équations en escalier obtenu est alors incompatible et, partant, est incompatible le système d'équations (1) de départ qui lui est équipotent. Mais si dans le premier membre de la dernière équation du système en escalier obtenu il y a des coefficients différents de zéro, alors le système en escalier obtenu prend la forme

$$
(2)\quad \begin{aligned}
\alpha'_{11}x_1 + \alpha'_{12}x_2 + \ldots + \alpha'_{1r}x_r + \ldots + \alpha'_{1n}x_n &= \beta'_1,\\
\alpha'_{22}x_2 + \ldots + \alpha'_{2r}x_r + \ldots + \alpha'_{2n}x_n &= \beta'_2,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\alpha'_{rr}x_r + \ldots + \alpha'_{rn}x_n &= \beta'_r,
\end{aligned}
$$

où les coefficients α'_{11}, α'_{22}, . . ., α'_{rr} sont différents de zéro. Le système (2) est compatible et équipotent au système initial (1).

A partir du système en escalier (2) passons par une série de transformations élémentaires au système d'équations en escalier

$$
(3)\quad \begin{aligned}
x_1 \qquad - \gamma_{1r+1}x_{r+1} - \ldots - \gamma_{1n}x_n &= \delta_1,\\
x_2 \qquad - \gamma_{2r+1}x_{r+1} - \ldots - \gamma_{2n}x_n &= \delta_2,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
x_r - \gamma_{rr+1}x_{r+1} - \ldots - \gamma_{rn}x_n &= \delta_r.
\end{aligned}
$$

Le système (3) est compatible et équipotent au système d'équations (1) initial. Si, de plus, $r = n$, le système d'équations (3) (et le système (1)) admet alors une solution unique $(\delta_1, \delta_2, \ldots, \delta_n)$. Mais si $r(A) = r(B) < n$, le système (3) est alors équipotent au système

$$
(4)\quad \begin{aligned}
x_1 &= \gamma_{1r+1}x_{r+1} + \ldots + \gamma_{1n}x_n + \delta_1,\\
x_2 &= \gamma_{2r+1}x_{r+1} + \ldots + \gamma_{2n}x_n + \delta_2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
x_r &= \gamma_{rr+1}x_{r+1} + \ldots + \gamma_{rn}x_n + \delta_r.
\end{aligned}
$$

Les équations du système (4) fournissent une expression explicite des variables $x_1, \ldots, x_r$ dites *principales* par l'intermédiaire des variables $x_{r+1}, \ldots, x_n$ dites *libres*. En attribuant dans les équations (4) aux variables libres des valeurs quelconques du corps des scalaires, on obtient les valeurs correspondantes des variables principales. On est ainsi en mesure d'obtenir toute solution particulière du système d'équations initial (1), puisqu'il est équipotent au système (4). C'est pourquoi le vecteur

$$
(5)\quad (\gamma_{1r+1}x_{r+1} + \ldots + \gamma_{1n}x_n + \delta_1, \ldots, \gamma_{rr+1}x_{r+1} + \ldots \\
\ldots + \gamma_{1n}x_n + \delta_r, x_{r+1}, \ldots, x_n)
$$

est appelé *solution générale du système d'équations* (1). Le vecteur (5) peut être écrit sous la forme

$$
(6)\quad x_{r+1}C_{r+1} + \ldots + x_nC_n + \delta,
$$

où $C_{r+1}, \ldots, C_n \in F^n$ et $\delta = (\delta_1, \ldots, \delta_r, 0, \ldots, 0)$ est la solution particulière du système (1). Le vecteur (6) est également nommé *solution générale du système* (1). On voit aisément que les vecteurs $C_{r+1}, \ldots, C_n$ constituent le système fondamental de solutions d'un système homogène d'équations associé au système (1).

L'ensemble $\{x_{r+1}C_{r+1} + \ldots + x_nC_n + \delta \mid x_{r+1}, \ldots, x_n \in F\}$ est l'ensemble de toutes les solutions du système d'équations (1).

Pour étudier la compatibilité du système donné d'équations linéaires (1) il faut réduire la matrice complète B du système par une série de transformations élémentaires sur les lignes à une matrice en escalier B'. Le système d'équations linéaires (1') à matrice complète B' est équipotent au système d'équations initial (1). Le système d'équations (1') est incompatible si et seulement si le rang des lignes de sa matrice fondamentale A' est inférieur au rang des lignes de la matrice complète B', c'est-à-dire si dans la dernière ligne de la matrice en escalier B' tous les éléments à part le dernier sont nuls.

Exercices

1. Démontrer qu'une matrice non nulle est équivalente par lignes à une et seulement à une matrice en escalier réduite.
2. Démontrer que la matrice A d'ordre $m \times n$ est équivalente par lignes à une matrice unité d'ordre $n \times n$ si et seulement si le rang de la matrice A vaut n.
3. Montrer que deux systèmes homogènes linéaires sur le corps $\mathcal{F}$ à variables $x_1, \ldots, x_n$ sont équipotents si et seulement si les matrices de ces systèmes sont équivalentes par lignes.
4. Soit $\mathcal{F}$ un corps fini composé de k éléments. Montrer qu'un système homogène donné d'équations linéaires sur le corps $\mathcal{F}$ à n variables possède k^{n-r} solutions, où r est le rang de la matrice du système donné d'équations.
5. Démontrer qu'un système compatible d'équations linéaires à matrice fondamentale non nulle n'est équipotent qu'à un seul et unique système en escalier réduit d'équations linéaires.
6. Démontrer que si deux systèmes compatibles d'équations linéaires sont équipotents, alors les systèmes homogènes d'équations linéaires qui leur sont associés sont également équipotents.
7. Démontrer que deux systèmes compatibles d'équations linéaires sur le corps $\mathcal{F}$ à variables $x_1, \ldots, x_n$ sont équipotents si et seulement si les matrices complètes de ces systèmes sont équivalentes par lignes.

CHAPITRE VI

MATRICES ET DÉTERMINANTS

§ 1. Opérations sur les matrices et leurs propriétés

Opérations sur les matrices. Partout dans ce chapitre $\mathcal{F} = \langle F, +, -, \cdot, 1 \rangle$ est un corps de choix fixé qu'on appellera *corps des scalaires*. Les éléments de l'ensemble F seront nommés *scalaires*.

Soient m et n des entiers positifs. Le tableau

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{bmatrix}$$

à éléments de F est appelé *matrice sur le corps* $\mathcal{F}$ ou *matrice* $m \times n$ sur $\mathcal{F}$; on note brièvement $\| \alpha_{ik} \|$ et l'on écrit $A = \| \alpha_{ik} \|$. Si $m = n$ la matrice A est une *matrice carrée* d'ordre n. L'ensemble de toutes les matrices $m \times n$ sur le corps $\mathcal{F}$ est noté $F^{m\times n}$. En particulier, l'ensemble de toutes les matrices carrées d'ordre n sur $\mathcal{F}$ est noté $F^{n\times n}$.

Conservons les notations précédentes pour les lignes et les colonnes de la matrice A : la i-ième ligne de la matrice A est notée A_i:

$$A_i = [\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{in}];$$

la k-ième colonne est notée A^k:

$$A^k = \begin{bmatrix} \alpha_{1k} \\ \alpha_{2k} \\ \vdots \\ \alpha_{nk} \end{bmatrix}.$$

Deux matrices $m \times n$ $A = \| \alpha_{ik} \|$ et $B = \| \beta_{ik} \|$ sont dites *égales* et l'on écrit $A = B$ si $\alpha_{ik} = \beta_{ik}$ pour tous indices i et k.

Une matrice est dite *nulle* et est notée O si tous ses éléments sont nuls.

On appelle *somme de deux matrices* $m \times n$ A *et* B la matrice $m \times n$ dont l'élément ik-ième est égal à $\alpha_{ik} + \beta_{ik}$, c'est-à-dire

$$A + B = \| \alpha_{ik} + \beta_{ik} \|.$$

13—01762

On appelle *produit du scalaire* λ *par la matrice* $A = \| \alpha_{ik} \|$ la matrice $m \times n$ $\| \lambda\alpha_{ik} \|$ notée λA :

$$\lambda A = \| \lambda\alpha_{ik} \|.$$

Pour la matrice $(-1) A$ on a l'égalité

$$A + (-1) A = 0.$$

Aussi la matrice $(-1) A$ est-elle également notée $-A$ et elle est appelée *matrice opposée à la matrice* A.

Soient $A \in F^{m\times n}$ et $B \in F^{n\times p}$:

$$A = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \dots & \dots & \dots \\ \alpha_{m1} & \dots & \alpha_{mn} \end{bmatrix}, \quad B = \begin{bmatrix} \beta_{11} & \dots & \beta_{1p} \\ \dots & \dots & \dots \\ \beta_{n1} & \dots & \beta_{np} \end{bmatrix}.$$

On admet ainsi que le nombre de colonnes de la matrice A est égal au nombre de lignes de la matrice B. Le *produit de la ligne* A_i *par la colonne* B^k se définit ainsi :

$$A_iB^k = [\alpha_{i1}, \dots, \alpha_{in}] \cdot \begin{bmatrix} \beta_{1k} \\ \vdots \\ \beta_{nk} \end{bmatrix} =$$

$$= \alpha_{i1}\beta_{1k} + \dots + \alpha_{in}\beta_{nk} = \sum_{j=1}^{n} \alpha_{ij}\beta_{jk}.$$

On appelle *produit des matrices* A *et* B la matrice $m \times p$ dont le ik-ième élément est égal à A_iB^k, c'est-à-dire

$$A \cdot B = \begin{bmatrix} A_1B^1 & A_1B^2 & \dots & A_1B^p \\ A_2B^1 & A_2B^2 & \dots & A_2B^p \\ \dots & \dots & \dots & \dots \\ A_mB^1 & A_mB^2 & \dots & A_mB^p \end{bmatrix}.$$

Bref, si A est la matrice $m \times n$ et B la matrice $n \times p$, alors AB est la matrice $m \times p$.

THÉORÈME 1.1. *Une multiplication des matrices est associative, c'est-à-dire pour toutes matrices* A, B *et* C $A(BC) = (AB)C$ *si les produits* AB *et* BC *existent.*

D é m o n s t r a t i o n. Par hypothèse, les produits AB et BC existent. On peut donc considérer que $A \in F^{m\times n}$, $B \in F^{n\times p}$, $C \in F^{p\times q}$. Donc les produits $A(BC)$ et $(AB)C$ existent et appartiennent à l'ensemble $F^{m\times q}$. Soient $H = A(BC)$, $H' = (AB)C$ et h_{ik}, h'_{ik} les ik-ièmes éléments des matrices H et H' respectivement.

Démontrons que $h_{ik} = h'_{ik}$ pour tous indices i et k. En effet,

$$h_{ik} = A_i (BC)^k = [\alpha_{i1}, \ldots, \alpha_{in}] \begin{bmatrix} B_1C^k \\ \vdots \\ B_nC^k \end{bmatrix} =$$

$$= \alpha_{i1}B_1C^k + \ldots + \alpha_{in}B_nC^k =$$

$$= \alpha_{i1} \sum_{s=1}^{p} \beta_{1s}\gamma_{sk} + \ldots + \alpha_{in} \sum_{s=1}^{p} \beta_{ns}\gamma_{sk} =$$

$$= \sum_{\substack{j=1,\ldots,n \\ s=1,\ldots,p}} \alpha_{ij}\beta_{js}\gamma_{sk};$$

$$h'_{ik} = (AB)_i C^k = [A_iB^1, \ldots, A_iB^p] \begin{bmatrix} \gamma_{1k} \\ \vdots \\ \gamma_{pk} \end{bmatrix} =$$

$$= A_iB^1\gamma_{1k} + \ldots + A_iB^p\gamma_{pk} =$$

$$= \Big(\sum_{j=1}^{n} \alpha_{ij}\beta_{j1}\Big) \gamma_{1k} + \ldots + \Big(\sum_{j=1}^{n} \alpha_{ij}\beta_{jp}\Big) \gamma_{pk} =$$

$$= \sum_{\substack{j=1,\ldots,n \\ s=1,\ldots,p}} \alpha_{ij}\beta_{js}\gamma_{sk}.$$

Par conséquent, $h_{ik} = h'_{ik}$ pour tous indices i et k, c'est-à-dire $A (BC) = (AB) C$. □

THÉORÈME 1.2. *Les opérations sur les matrices sont douées des propriétés suivantes*:

(1) *l'algèbre* $\langle F^{m\times n}, +, - \rangle$ *est un groupe abélien*;

(2) $\alpha (A + B) = \alpha A + \alpha B$ $(\alpha,\ \beta \in F,\ A,\ B \in F^{m\times n})$;

(3) $(\alpha + \beta) A = \alpha A + \beta A$;

(4) $(\alpha\beta) A = \alpha (\beta A)$;

(5) $1 \cdot A = A$;

(6) *la multiplication des matrices est associative*;

(7) *la multiplication des matrices est distributive par rapport à l'addition, c'est-à-dire* $A (B + C) = AB + AC$ *si le produit* AB *et la somme* $B + C$ *existent, et* $(B + C) A = BA + CA$ *si le produit* BA *et la somme* $B + C$ *existent*;

(8) *pour tout scalaire* λ *et toutes matrices* A, B *on a*

$$\lambda (AB) = (\lambda A) B = A (\lambda B)$$

si le produit AB *existe.*

D é m o n s t r a t i o n. Les propriétés (1)-(5) se démontrent de la même façon que les propriétés correspondantes de l'addition des

vecteurs et de la multiplication par un scalaire des vecteurs des espaces vectoriels arithmétiques.

Selon le théorème 1.1 la multiplication des matrices est associative.

Démontrons que la multiplication des matrices est distributive par rapport à l'addition. Soient $A \in F^{m\times n}$, B, $C \in F^{n\times p}$. On vérifie sans peine que AB, $AC \in F^{m\times p}$, $B + C \in F^{n\times p}$. D'où il s'ensuit que $A\,(B + C)$ et $AB + AC$ sont des matrices $m \times p$. Montrons que les ik-ièmes éléments de ces matrices sont égaux, c'est-à-dire que $A_i\,(B + C)^k = A_iB^k + A_iC^k$. En effet,

$$A_i\,(B+C)^k = \sum_{j=1,\ldots,n} \alpha_{ij}\,(\beta_{jk}+\gamma_{jk});$$

$$A_iB^k + A_iC^k = \sum_{j=1,\ldots,n} \alpha_{ij}\beta_{jk} + \sum_{j=1,\ldots,n} \alpha_{ij}\gamma_{jk} = \sum_{j=1,\ldots,n} \alpha_{ij}\,(\beta_{jk}+\gamma_{jk}).$$

Par conséquent, $A\,(B + C) = AB + BC$. On démontre de façon analogue que $(B + C)A = BA + CA$ si le produit BA et la somme $B + C$ existent.

Pour démontrer la propriété (8) cherchons les ik-ièmes éléments des matrices $\lambda\,(AB)$, $(\lambda A)B$, $A\,(\lambda B)$:

$$\lambda\,(A_iB^k) = \lambda \sum_{j=1}^{n} \alpha_{ij}\beta_{jk}; \quad (\lambda A_i)\,B^k = \sum_{j=1}^{n} (\lambda\alpha_{ij})\,\beta_{jk};$$

$$A_i\,(\lambda B^k) = \sum_{j=1}^{n} \alpha_{ij}\,(\lambda\beta_{jk}).$$

Ces trois expressions sont égales entre elles en vertu des propriétés de l'addition et de la multiplication des scalaires. Donc, $\lambda\,(AB) = (\lambda A)\,B = A\,(\lambda B)$. □

Transposition du produit des matrices. Soit $A = \|\alpha_{ik}\|$ la matrice $m \times n$ sur le corps $\mathcal{F}$. On appelle alors *matrice transposée* de A la matrice $n \times m$ $\|\beta_{ik}\|$ telle que $\beta_{ik} = \alpha_{ik}$, et elle est notée ${}^tA$. On obtient donc la matrice transposée en échangeant les lignes et les colonnes de la matrice donnée. En particulier,

$$({}^tA)^i = {}^t[\alpha_{i1}, \ldots, \alpha_{in}] = \begin{bmatrix}\alpha_{i1}\\ \vdots\\ \alpha_{in}\end{bmatrix};$$

$$({}^tA)_k = {}^t\begin{bmatrix}\alpha_{1k}\\ \vdots\\ \alpha_{mk}\end{bmatrix} = [\alpha_{1k}, \ldots, \alpha_{mk}].$$

THÉORÈME 1.3. *Si le produit AB des matrices A et B existe, il existe aussi un produit ${}^tB\cdot{}^tA$ et ${}^t(AB) = {}^tB\cdot{}^tA$.*

D é m o n s t r a t i o n. Supposons que $A \in F^{m\times n}$ et $B \in F^{n\times p}$. Alors si $C = AB$, $AB \in F^{m\times p}$ et ${}^t(AB) \in F^{p\times m}$. De plus, ${}^tB \in F^{p\times n}$ et ${}^tA \in F^{p\times n}$. Par conséquent, le produit ${}^tB\cdot{}^tA$ existe et ${}^tB{}^tA \in \in F^{p\times m}$. Les matrices $C = {}^t(AB)$ et $C' = {}^tB\cdot{}^tA$ sont ainsi des matrices $p \times m$. Vérifions que les ik-ièmes éléments c_{ik} et c'_{ik} de ces matrices sont égaux. En effet,

$$c_{ik} = A_kB^i = [\alpha_{k1}, \ldots, \alpha_{kn}] \begin{bmatrix} \beta_{1i} \\ \vdots \\ \beta_{ni} \end{bmatrix} = \alpha_{k1}\beta_{1i} + \ldots + \alpha_{kn}\beta_{ni};$$

d'autre part,

$$c'_{ik} = ({}^tB)_i\,({}^tA)^k = [\beta_{1i}, \ldots, \beta_{ni}] \begin{bmatrix} \alpha_{k1} \\ \vdots \\ \alpha_{kn} \end{bmatrix} =$$

$$= \alpha_{k1}\beta_{1i} + \ldots + \alpha_{kn}\beta_{ni}.$$

Par conséquent, $c_{ik} = c'_{ik}$ pour tous indices i et k, c'est-à-dire ${}^t(AB) = {}^tB\cdot{}^tA$. □

Exercices

1. Soit $A = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$. Chercher A^n pour tout entier positif n.

2. Démontrer que si pour les matrices A et B les produits AB et BA existent et $AB = BA$, les matrices A et B sont carrées et possèdent un même ordre.

3. Soient A et B des matrices carrées de même ordre et $AB = BA$. Démontrer que pour tout entier positif n est vraie la formule

$$(A+B)^n = A^n + n\cdot A^{n-1}\cdot B + \frac{n(n-1)}{2} A^{n-2}\cdot B^2 + \ldots + B^n.$$

4. Montrer que l'opération de transposition est douée des propriétés suivantes:

(a) ${}^t(A+B) = {}^tA + {}^tB$; (b) ${}^t(\lambda A) = \lambda\cdot{}^tA$, où λ est un scalaire; (c) ${}^t(A^{-1}) = ({}^tA)^{-1}$; (d) ${}^t(ABC) = {}^tC\cdot{}^tB\cdot{}^tA$ si le produit ABC existe.

5. Une matrice carrée A est dite *symétrique* si $A = {}^tA$. Montrer que si A est une matrice carrée, la matrice $A + {}^tA$ est symétrique.

6. Une matrice carrée A est dite *symétrique gauche* si $A = -{}^tA$. Démontrer que toute matrice carrée peut être représentée, et cela de façon unique, sous forme de somme de matrices symétrique et symétrique gauche.

7. Démontrer que des transformations élémentaires sur les colonnes d'une matrice peuvent être réalisées au moyen d'une multiplication de la matrice à droite par des matrices élémentaires correspondantes.

§ 2. Matrices inversibles

Matrices inversibles. Soit A une matrice $n \times n$ sur le corps des scalaires $\mathcal{F}$. Si E est une matrice unité $n\times n$, on a alors

(1) $AE = A = EA$.

Une matrice carrée est dite *inversible* s'il existe une matrice B satisfaisant aux conditions

$$(2)\quad AB = E, \qquad BA = E.$$

La matrice B satisfaisant à ces conditions est dite *inverse de* A. Les matrices A et B sont appelées *mutuellement inverses.*

PROPOSITION 2.1. *Si la matrice A est inversible, il n'existe alors qu'une seule matrice inverse de A.*

Démonstration. Supposons que B et C sont des matrices inverses de A. On a alors $AC = E = BA$ et $B = BE = B(AC) = (BA)C = E \cdot C = C$, c'est-à-dire que $B = C$. □

Si la matrice A est inversible, alors la matrice inverse de A est notée A^{-1}. Ainsi, pour toute matrice inversible on a les égalités

$$(3)\quad AA^{-1} = E, \qquad A^{-1}A = E.$$

L'ensemble de toutes les matrices inversibles $n \times n$ sur le corps $\mathcal{F}$ est noté $GL(n, \mathcal{F})$.

THÉORÈME 2.2. *L'algèbre $\langle GL(n, \mathcal{F}), \cdot, ^{-1}\rangle$ est un groupe.*

Démonstration. La matrice unité E est, évidemment, inversible et, en raison de (1), est un élément neutre.

Si la matrice A est inversible, alors en vertu de (2) la matrice A^{-1} est également inversible.

L'ensemble $GL(n, \mathcal{F})$ des matrices inversibles $n \times n$ est également fermé par rapport à la multiplication. En effet, si $A, B \in GL(n, \mathcal{F})$, on a alors

$$(AB)(B^{-1}A^{-1}) = E = (B^{-1}A^{-1})(AB),$$

c'est-à-dire que la matrice AB est inversible sur $\mathcal{F}$ et, partant, appartient à l'ensemble $GL(n, \mathcal{F})$.

Enfin, selon le théorème 1.1, la multiplication des matrices est associative. □

COROLLAIRE 2.3. *Un produit de tout nombre des matrices inversibles est une matrice inversible.*

Matrices élémentaires. Introduisons la notion de matrice élémentaire.

DÉFINITION. La matrice carrée obtenue à partir de la matrice unité par transformation élémentaire régulière sur des lignes (des colonnes) est appelée *matrice élémentaire* associée à cette transformation.

C'est ainsi que sont des matrices élémentaires du second ordre les matrices

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \quad \begin{bmatrix}1 & \lambda\\ 0 & 1\end{bmatrix}, \quad \begin{bmatrix}\lambda & 0\\ 0 & 1\end{bmatrix}, \quad \begin{bmatrix}1 & 0\\ 0 & \lambda\end{bmatrix}, \quad \begin{bmatrix}1 & 0\\ \lambda & 1\end{bmatrix},$$

où λ est un scalaire non nul quelconque.

La matrice élémentaire s'obtient à partir d'une matrice unité E par l'une des transformations régulières suivantes:

1) la multiplication de la ligne (de la colonne) de la matrice E par un scalaire différent de zéro;

2) l'addition (ou la soustraction) à une ligne (colonne) quelconque de la matrice E d'une autre ligne (colonne) multipliée par un scalaire.

Désignons par $E_{\lambda(i)}$ la matrice obtenue à partir de la matrice E après multiplication de la i-ième ligne par un scalaire λ non nul:

$$E_{\lambda(i)} = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & \lambda & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{bmatrix}.$$

Désignons par $E_{(i)+\lambda(k)}$ ($E_{(i)-\lambda(k)}$) la matrice obtenue à partir de la matrice E après addition (soustraction) à la i-ième ligne de la k-ième ligne multipliée par λ:

$$E_{(i)+\lambda(k)} = \begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & \lambda & \\ & & & \ddots & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{bmatrix}; \quad E_{(i)-\lambda(k)} = \begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & -\lambda & \\ & & & \ddots & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{bmatrix}.$$

On notera E_φ la matrice obtenue à partir de la matrice unité E après application de la transformation élémentaire φ sur les lignes; ainsi E_φ est la matrice correspondant à la transformation φ.

Considérons quelques propriétés des matrices élémentaires.

PROPRIETE 2.1. *Toute matrice élémentaire est inversible. Une matrice inverse de la matrice élémentaire est une matrice élémentaire.*

D é m o n s t r a t i o n. Une vérification directe montre que pour tout scalaire λ différent de zéro et i et k quelconques on a les égalités

$$E_{\lambda(i)}E_{\lambda^{-1}(i)} = E = E_{\lambda^{-1}(i)}E_{\lambda(i)};$$

$$E_{(i)+\lambda(k)}E_{(i)-\lambda(k)} = E = E_{(i)-\lambda(k)}E_{(i)+\lambda(k)}.$$

Sur la base de ces égalités on conclut qu'on a la propriété 2.1. □

PROPRIETE 2.2. *Un produit des matrices élémentaires est une matrice inversible.*

Cette propriété découle directement de la propriété 2.1. et du corollaire 2.3.

PROPRIETE 2.3. *Si une transformation élémentaire régulière par lignes φ fait passer la matrice $m \times n$ A en la matrice B, on a alors $B = E_\varphi A$ ($E_\varphi \in F^{m\times m}$). La réciproque est également vraie.*

D é m o n s t r a t i o n. Si φ est une multiplication de la i-ième ligne $A = \| \alpha_{ik} \|$ par un scalaire non nul λ, on a

$$E_{\lambda(i)}A = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \cdot & \cdot & \cdot \\ \lambda\alpha_{i1} & \dots & \lambda\alpha_{in} \\ \cdot & \cdot & \cdot \\ \alpha_{m1} & \dots & \alpha_{mn} \end{bmatrix},$$

c'est-à-dire $B = E_{\varphi}A$. Mais si $E_{\varphi} = E_{(i)+\lambda(k)}$, alors

$$E_{(i)+\lambda(k)}A = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \cdot & \cdot & \cdot \\ \alpha_{i1}+\lambda\alpha_{k1} & \dots & \alpha_{in}+\lambda\alpha_{kn} \\ \cdot & \cdot & \cdot \\ \alpha_{m1} & \dots & \alpha_{mn} \end{bmatrix},$$

c'est-à-dire $B = E_{(i)+\lambda(k)} \cdot A$.

On vérifie sans peine que l'affirmation inverse est également vraie. □

PROPRIETE 2.4. *Si la matrice C est obtenue à partir de la matrice A par une série de transformations élémentaires régulières par lignes* $\varphi_1, \dots, \varphi_s$, *on a alors* $C = E_{\varphi_s} \dots E_{\varphi_1} \cdot A$. *La réciproque est également vraie.*

D é m o n s t r a t i o n. Selon la propriété 2.3 la transformation φ_1 fait passer la matrice A en la matrice $E_{\varphi_1} \cdot A$, φ_2 fait passer la matrice $E_{\varphi_1} \cdot A$ en la matrice $E_{\varphi_2}E_{\varphi_1} \cdot A$, etc. Enfin, φ_s fait passer la matrice $E_{\varphi_{s-1}} \dots E_{\varphi_1} \cdot A$ en la matrice $E_{\varphi_s}E_{\varphi_{s-1}} \dots E_{\varphi_1} \cdot A$. Par conséquent, $C = E_{\varphi_s} \dots E_{\varphi_2}E_{\varphi_1} \cdot A$.

On vérifie aisément que la réciproque est également vraie.

Conditions d'inversibilité de la matrice. Pour démontrer le théorème 2.8 on a besoin de trois lemmes suivants.

LEMME 2.4. *Une matrice carrée à ligne (colonne) dont les éléments sont nuls est irréversible.*

D é m o n s t r a t i o n. Soit A une matrice carrée dont la ligne est à éléments nuls, B étant une matrice quelconque, $A, B \in F^{n \times n}$. Soit A_i la ligne à éléments nuls de la matrice A, on a alors

$$(AB)_i = [A_iB^1, \dots, A_iB^n] = [0, \dots, 0],$$

c'est-à-dire que la i-ième ligne de AB ne possède que des éléments nuls. Donc la matrice A est irréversible. □

LEMME 2.5. *Si les lignes d'une matrice carrée sont linéairement dépendantes, la matrice est alors irréversible.*

D é m o n s t r a t i o n. Soit A une matrice carrée aux lignes linéairement dépendantes. Il existe alors une série de transformations élémentaires régulières par lignes faisant passer A en une matrice en escalier; soit $\varphi_1, \dots, \varphi_s$ cette série. Selon la propriété 2.4 des

matrices élémentaires on a l'égalité

(1) $E_{\varphi_s} \ldots E_{\varphi_1} \cdot A = C$,

où C est une matrice avec ligne à éléments partout nuls. Par conséquent, selon le lemme 2.4 la matrice C est irréversible. Mais si, par contre, la matrice A était inversible, le produit à gauche dans l'égalité (1) serait alors une matrice inversible, comme produit de matrices inversibles (voir corollaire 2.3), ce qui est impossible. Donc, la matrice A est irréversible. □

COROLLAIRE 2.6. *Si une matrice carrée est inversible, ses lignes sont alors linéairement indépendantes.*

LEMME 2.7. *Une matrice carrée à lignes linéairement indépendantes peut être représentée sous forme d'un produit de matrices élémentaires.*

Démonstration. Soit A une matrice carrée à lignes linéairement indépendantes. Il existe une série de transformations élémentaires régulières par lignes $\varphi_1, \ldots, \varphi_s$ faisant passer la matrice A en la matrice unité E. Selon la propriété 2.4 des matrices élémentaires, il s'ensuit que $E_{\varphi_s} \ldots E_{\varphi_1} \cdot A = E$. Donc, $A = E_{\varphi_s}^{-1} \ldots E_{\varphi_1}^{-1}$, où, selon la propriété 2.1 des matrices élémentaires, les facteurs $E_{\varphi_1}^{-1}, \ldots, E_{\varphi_s}^{-1}$ sont des matrices élémentaires. □

THÉORÈME 2.8. *Pour toute matrice carrée A ($A \in F^{n \times n}$) les trois affirmations suivantes sont équipotentes:*

(a) *la matrice A est inversible;*

(b) *les lignes (colonnes) de la matrice A sont linéairement indépendantes;*

(c) *la matrice A peut se représenter sous forme d'un produit des matrices élémentaires.*

Démonstration. Selon le corollaire du lemme 2.5, (b) s'ensuit de (a). Ensuite, selon le lemme 2.7 (c) s'ensuit de (b). Enfin, en vertu de la propriété 2.2 des matrices élémentaires et du corollaire 2.3, (a) dérive de (c). Donc, les affirmations (a), (b) et (c) sont équipotentes. □

Calcul de la matrice inverse. On est maintenant en mesure de fonder une règle très simple de calcul de la matrice inverse.

THÉORÈME 2.9. *Si par une série de transformations élémentaires régulières par lignes on fait passer une matrice carrée A en une matrice unité E, la matrice A est alors inversible et cette même série des transformations fait passer la matrice E en la matrice A^{-1}.*

Démonstration. Supposons que $\varphi_1, \ldots, \varphi_s$ est la série des transformations faisant passer la matrice carrée A en la matrice unité E. Alors, selon la propriété 2.4 des matrices élémentaires,

$$E = E_{\varphi_s} \ldots E_{\varphi_1} A.$$

En vertu de la proposition 2.1 il s'ensuit que la matrice A est inversible et

$$A^{-1} = E_{\varphi_s} \ldots E_{\varphi_1} E.$$

Selon la propriété 2.4 des matrices élémentaires, il dérive de la dernière égalité que la série de transformations élémentaires par lignes $\varphi_1, \ldots, \varphi_s$ transforme la matrice E en la matrice A^{-1}. □

Le théorème 2.9 permet de formuler la règle suivante d'obtention de la matrice inverse. *Pour trouver la matrice inverse de la matrice A d'ordre $n \times n$, il faut faire passer la matrice rectangulaire $n \times 2n$ $(A \mid E)$ en une matrice de la forme $(E \mid C)$ par une série de transformations élémentaires régulières par lignes; la matrice C ainsi obtenue est inverse de la matrice A.*

Notation et résolution du système de *n* équations linéaires à *n* variables sous forme matricielle. Considérons un système d'équations linéaires

$$\begin{aligned} \alpha_{11}x_1 + \ldots + \alpha_{1n}x_n &= \beta_1, \\ \ldots\ldots\ldots\ldots\ldots & \\ \alpha_{n1}x_1 + \ldots + \alpha_{nn}x_n &= \beta_n \end{aligned} \tag{I}$$

sur le corps $\mathcal{F}$. En introduisant les notations

$$A = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \ldots & \ldots & \ldots \\ \alpha_{n1} & \ldots & \alpha_{nn} \end{bmatrix}, \quad b = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}, \quad \mathcal{X} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix},$$

on est en mesure d'écrire le système (I) sous forme d'une équation matricielle

$$A\mathcal{X} = b. \tag{2}$$

On voit aussitôt que l'équation (2) est équipotente au système d'équations (I). Elle est dite *forme matricielle d'écriture du système d'équations* (I).

THÉORÈME 2.10. *Si les lignes de la matrice A sont linéairement indépendantes, le vecteur $A^{-1}b$ est alors l'unique solution de l'équation* (2).

Démonstration. Supposons qu'un vecteur colonne $\mathcal{X}_0$ est la solution de l'équation (2), c'est-à-dire que $A\mathcal{X}_0 = b$. En multipliant à gauche les deux membres de l'égalité $A\mathcal{X}_0 = b$ par A^{-1}, on obtient

$$\mathcal{X}_0 = A^{-1} \cdot b. \tag{3}$$

Ainsi, ou bien l'équation (2) possède une solution $A^{-1}b$, ou bien elle n'en possède pas. Toutefois, l'égalité $A(A^{-1} \cdot b) = b$ montre que le vecteur $A^{-1} \cdot b$ est une solution de l'équation (2). Par conséquent, le vecteur $A^{-1} \cdot b$ est l'unique solution de l'équation (2). □

COROLLAIRE 2.11. *Si les lignes de la matrice fondamentale A du système* (I) *sont linéairement indépendantes, le système est alors compatible et le vecteur $A^{-1} \cdot b$ est la solution unique de ce système.*

Exercices

1. Soit $A = \| \alpha_{ij} \|$ une matrice carrée d'ordre n (sur le corps $\mathscr{F}$). Notons E_{ik} (i, $k = 1, \ldots, n$) la matrice dont la i-ième ligne et la k-ième colonne ont 1 pour élément, les éléments restants étant nuls. Montrer que

$$(*) \quad AE_{ik} = \alpha_{1i}E_{1k} + \ldots + \alpha_{ni}E_{nk}, \quad E_{ik}A = \alpha_{k1}E_{i1} + \ldots + \alpha_{kn}E_{in}.$$

2. Sur la base de l'égalité (*) démontrer que la matrice A est permutable avec chacune des matrices E_{ik} si et seulement si A est de la forme λE, où $\lambda \in F$.

3. Utilisant le résultat du problème précédent montrer que la matrice A est permutable avec une quelconque matrice carrée d'ordre n (sur le corps $\mathscr{F}$) si et seulement si $A = \lambda E$, où $\lambda \in F$.

4. Soit A une matrice carrée d'ordre n. Démontrer que la matrice A est permutable avec une matrice diagonale quelconque d'ordre n si et seulement si la matrice A est elle-même diagonale.

5. Soit A une matrice diagonale, tous les éléments de la diagonale principale étant différents l'un de l'autre. Montrer que toute matrice qui est permutable avec A est aussi diagonale.

6. Montrer qu'une matrice carrée A d'ordre n permutable avec une matrice quelconque symétrique du même ordre est une *matrice scalaire*, c'est-à-dire que $A = \lambda E$, où λ est un scalaire et E une matrice unité d'ordre n.

7. Soit A une matrice carrée d'ordre n (sur le corps $\mathscr{F}$). Démontrer que l'ensemble de toutes les matrices (sur $\mathscr{F}$), permutables avec la matrice A, est fermé par rapport à l'addition et par rapport à la multiplication.

§ 3. Permutations

Permutations. Groupe des permutations. Considérons les permutations de l'ensemble $M = \{1, \ldots, n\}$, où n est un nombre naturel autre que zéro. On appelle *permutation de l'ensemble* M l'application injective de l'ensemble M sur lui-même.

Toute application φ de l'ensemble M sur lui-même se note de façon commode sous forme de tableau

$$\varphi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \varphi(1) & \varphi(2) & \ldots & \varphi(n) \end{pmatrix}.$$

L'ordre des nombres dans la première ligne a peu d'importance, et on peut le varier de façon quelconque. Toutefois, il faut veiller à ce que pour tout k le nombre $\varphi(k)$ soit placé immédiatement au-dessous de k.

L'ensemble de toutes les permutations de l'ensemble M sera noté S_n; les éléments de cet ensemble sont nommés *permutations d'indice n*.

Si $\varphi \in S_n$, alors: (1) φ est une application injective, c'est-à-dire que pour tous $i, k \in M$ il s'ensuit de $\varphi(i) = \varphi(k)$ que $i = k$; (2) φ est une application de M sur lui-même, c'est-à-dire $\{\varphi(1), \ldots, \varphi(n)\} = \{1, \ldots, n\}$. M étant un ensemble fini, de la condition (1) se déduit la condition (2), et réciproquement.

Le produit $\varphi\psi$ de deux permutations φ et ψ de l'ensemble M se définit comme une composition d'applications φ et ψ ($\varphi\psi = \varphi \cdot \psi$)

Donc, par définition,

$$\varphi\psi(i) = \varphi(\psi_{(i)}), \qquad i = 1, \ldots, n.$$

Une composition de toutes deux applications injectives de l'ensemble M sur lui-même est une application injective de l'ensemble M sur lui-même. Par conséquent, pour deux permutations quelconques φ, ψ de S_n, on a $\varphi\psi \in S_n$.

Notons par ε l'application identique de l'ensemble M sur lui-même :

$$\varepsilon(i) = i, \quad i = 1, \ldots, n, \text{ c'est-à-dire } \varepsilon = \begin{pmatrix} 1 & 2 \ldots n \\ 1 & 2 \ldots n \end{pmatrix}.$$

On constate aisément que pour toute permutation φ de S_n $\varphi\varepsilon = \varepsilon\varphi = \varphi$, c'est-à-dire que ε est un élément neutre par rapport à la multiplication.

Si φ est une permutation de l'ensemble M, φ^{-1} est également une permutation de l'ensemble M et $\varphi\varphi^{-1} = \varepsilon = \varphi^{-1}\varphi$. De plus,

$$\varphi^{-1} = \begin{pmatrix} \varphi(1) & \ldots & \varphi(n) \\ 1 & \ldots & n \end{pmatrix} = \begin{pmatrix} 1 & \ldots & n \\ \varphi^{-1}(1) & \ldots & \varphi^{-1}(n) \end{pmatrix}.$$

THÉORÈME 3.1. *L'algèbre* $\langle S_n, \cdot, ^{-1}\rangle$ *est un groupe.*

Démonstration. On a établi plus haut que l'ensemble S_n est fermé aux opérations principales $\cdot$, $^{-1}$. Selon le théorème 2.3, une composition des fonctions est associative. Une permutation identique ε est un élément neutre par rapport à la multiplication et, pour toute permutation φ de S_n, on a l'égalité $\varphi\varphi^{-1} = \varepsilon = \varphi^{-1}\varphi$. Ainsi, l'algèbre $\langle S_n, \cdot, ^{-1}\rangle$ est donc un groupe. □

DÉFINITION. Le groupe $\langle S_n, \cdot, ^{-1}\rangle$ est dit *groupe symétrique d'indice* n et est noté $\mathscr{S}_n$. L'élément ε est nommé *élément unité de ce groupe.*

Permutations paires et impaires. Soit donnée une permutation de l'ensemble $M = \{1, \ldots, n\}$

$$\varphi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \varphi(1) & \varphi(2) & \ldots & \varphi(n) \end{pmatrix}.$$

Considérons un couple non ordonné $\{i, k\}$ d'éléments différents de l'ensemble M. Le couple $\{i, k\}$ est dit *régulier* relativement à la permutation φ si les différences $i - k$ et $\varphi(i) - \varphi(k)$ sont affectées du même signe. On dit que le couple $\{i, k\}$ est *irrégulier* relativement à la permutation φ ou y constitue une *inversion* si les différences $i - k$ et $\varphi(i) - \varphi(k)$ sont munies de signes opposés. C'est ainsi, par exemple, que dans la permutation identique $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ il n'y a pas d'inversions. Dans la permutation $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ on n'a qu'une inversion.

Dans la permutation $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ il y a deux inversions.

La permutation est dite *paire* si elle comporte un nombre pair d'inversions ; elle est dite *impaire* si le nombre d'inversions est impair. C'est ainsi, par exemple, qu'une permutation identique est paire.

La permutation φ de la forme

$$\begin{pmatrix} 1 \dots i \dots k \dots n \\ 1 \dots k \dots i \dots n \end{pmatrix}$$

est nommée *transposition*. Autrement dit, la permutation φ est appelée *transposition* s'il existe un couple $\{i, k\}$ d'éléments différents de M satisfaisant aux conditions

(1) $\varphi(i) = k, \; \varphi(k) = i, \; \varphi(s) = s$ pour chaque $s \in M \setminus \{i, k\}$.

LEMME 3.2. *Toute transposition est une permutation impaire.*

Démonstration. Soit φ une transposition faisant passer i en k $(i \neq k)$, c'est-à-dire satisfaisant aux conditions (1). Posons que $i < k$. On voit sans peine que le couple $\{s, t\} \subset M$ peut constituer une inversion si l'un au moins des éléments est i ou k ; dans le cas contraire les deux différences $s - t$ et $\varphi(s) - \varphi(t)$ coïncident.

Si $i < s$ ou $k < s$, il n'y a pas d'inversions parmi les couples $\{s, i\}$ et $\{k, s\}$ vu que les deux différences sont négatives.

Si $i < s \leqslant k$, parmi les couples $\{i, s\}$ sont des inversions les couples suivants : $\{i, i+1\}, \dots, \{i, k\}$, en tout $k - i$ inversions.

Si $i < s < k$, parmi les couples $\{s, k\}$ sont des inversions les couples $\{i+1, k\}, \dots, \{k-1, k\}$; il y a au total $k - i - 1$ inversions.

Bref, la transposition φ comporte au total $(k - i) + (k - i - 1) = 2(k - i) - 1$ inversions, et, par suite, φ est une permutation impaire. □

Signature d'une permutation. La signature de tout nombre rationnel a se définit de la façon suivante :

$$\operatorname{sing}(a) = \begin{cases} 1 \text{ pour } a > 0, \\ 0 \text{ pour } a = 0, \\ -1 \text{ pour } a < 0. \end{cases}$$

On voit aussitôt que *pour tous nombres rationnels a et b, on a*

$$\operatorname{sign}(ab) = \operatorname{sign}(a) \cdot \operatorname{sign}(b).$$

Cette propriété de la signature est appelée *propriété de multiplicativité* et elle sera utilisée pour la démonstration du lemme 3.3.

Notons sgn l'application de l'ensemble S_n dans l'ensemble

$\{1, -1\}$ définie par l'égalité:

$$\operatorname{sgn} \varphi = \begin{cases} 1, & \text{si } \varphi \text{ est une permutation paire,} \\ -1, & \text{si } \varphi \text{ est une permutation impaire.} \end{cases}$$

On voit sans peine que la signature ($\operatorname{sgn} \varphi$) de la permutation φ est égale au produit des signatures de tous les nombres $\frac{i-k}{\varphi(i)-\varphi(k)}$ correspondant à tous les couples possibles $\{i, k\}$ de divers éléments de l'ensemble M, c'est-à-dire que

$$\operatorname{sgn} \varphi = \prod_{\substack{\{i,\, k\} \subset M \\ i \neq k}} \operatorname{sign} \frac{i-k}{\varphi(i)-\varphi(k)}.$$

Lemme 3.3. *La signature d'un produit de deux permutations est le produit des signatures de ces permutations, c'est-à-dire*

(1) $\operatorname{sgn}(\varphi\psi) = \operatorname{sgn} \varphi \cdot \operatorname{sgn} \psi \quad (\varphi, \psi \in S_n)$.

Démonstration. On peut représenter la permutation $\varphi = \begin{pmatrix} \psi(1) & \dots & \psi(n) \\ \varphi\psi(1) & \dots & \varphi\psi(n) \end{pmatrix}$; donc,

$$\operatorname{sgn} \varphi = \prod_{\substack{\{i,\, k\} \subset M \\ i \neq k}} \operatorname{sign} \frac{\psi(i)-\psi(k)}{\varphi\psi(i)-\varphi\psi(k)};$$

par conséquent, on a

(2) $$\operatorname{sgn} \varphi \cdot \operatorname{sgn} \psi = \prod_{\substack{\{i,\, k\} \subset M \\ i \neq k}} \operatorname{sign} \frac{\psi(i)-\psi(k)}{\varphi\psi(i)-\varphi\psi(k)} \times \\ \times \prod_{\substack{\{i,\, k\} \subset M \\ i \neq k}} \operatorname{sign} \frac{i-k}{\psi(i)-\psi(k)}.$$

En vertu de la propriété de multiplicativité de la signature

$$\operatorname{sign} \frac{\psi(i)-\psi(k)}{\varphi\psi(i)-\varphi\psi(k)} \cdot \operatorname{sign} \frac{i-k}{\psi(i)-\psi(k)} = \\ = \operatorname{sign} \left(\frac{\psi(i)-\psi(k)}{\varphi\psi(i)-\varphi\psi(k)} \cdot \frac{i-k}{\psi(i)-\psi(k)} \right) = \operatorname{sign} \frac{i-k}{\varphi\psi(i)-\varphi\psi(k)}.$$

Aussi s'ensuit-il de (2) que

$$\operatorname{sgn} \varphi \cdot \operatorname{sgn} \psi = \prod_{\substack{\{i,\, k\} \subset M \\ i \neq k}} \operatorname{sign} \frac{i-k}{\varphi\psi(i)-\varphi\psi(k)} = \operatorname{sgn}(\varphi\psi). \ \square$$

Théorème 3.4. *La signature d'une permutation (fonction* sgn) *est douée des propriétés suivantes:*

(1) *la fonction* sgn *est multiplicative, c'est-à-dire* $\operatorname{sgn}(\varphi\psi) = \operatorname{sgn} \varphi \cdot \operatorname{sgn} \psi$ *pour tous* φ, ψ *de* S_n;

(2) *la signature de la transposition vaut* (-1);
(3) *les permutations inverses entre elles ont une même signature*;
(4) *si* τ *est une transposition et* φ *une permutation quelconque de* S_n, *on a alors* $\operatorname{sgn}(\tau\varphi) = \operatorname{sgn}(\varphi\tau) = -\operatorname{sgn}\varphi$.

Démonstration. La propriété (1) se vérifie à partir du lemme 3.3. La propriété (2) découle directement du lemme 3.2. En vertu de la propriété (1),

$$\operatorname{sgn}(\varphi\varphi^{-1}) = \operatorname{sgn}\varphi \cdot \operatorname{sgn}\varphi^{-1} = \operatorname{sgn}\varepsilon = 1$$

pour toute permutation φ. Par conséquent, $\operatorname{sgn}\varphi = \operatorname{sgn}\varphi^{-1}$. La propriété (4) découle directement des propriétés (1) et (2). □

COROLLAIRE 3.5. *Le produit de deux (ou d'un nombre pair) de permutations de même parité est une permutation paire.*

COROLLAIRE 3.6. *Le produit de deux permutations de parité différente est une permutation impaire.*

Exercices

1. Démontrer qu'il existe $n!$ permutations d'un ensemble composé de n éléments.
2. Montrer que si $n > 1$ le nombre de permutations paires de l'ensemble $\{1, 2, \ldots, n\}$ est égal au nombre de permutations impaires.
3. Démontrer que l'ensemble de toutes les permutations paires de S_n est clos par rapport à la multiplication et à l'opération d'obtention de l'inverse de l'élément.
4. Montrer que chaque permutation de S_n pour $n > 1$ peut être représentée sous forme d'un produit de transpositions de l'aspect $(k, k+1)$, où $1 \leqslant k < n$.
5. Montrer que chaque permutation de S_n pour $n > 1$ peut être représentée sous forme d'un produit de transpositions de l'aspect $(1, k)$, où $1 < k \leqslant n$.

§ 4. Déterminants

Déterminant d'une matrice carrée. Soit $\mathscr{F}$ un anneau commutatif ou un corps dont les éléments seront nommés *scalaires*. Soit

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn} \end{bmatrix}$$

une matrice sur $\mathscr{F}$, $A \in F^{n \times n}$. Soit S_n l'ensemble de toutes les permutations de l'ensemble $\{1, \ldots, n\}$.

Considérons l'ensemble $M(A)$ de tous les produits d'éléments de la matrice A pris par un de chaque ligne et colonne. Tout élément de l'ensemble $M(A)$ comporte n facteurs et peut être écrit ainsi:

(1) $a_{1i_1} \cdot a_{2i_2} \cdot \ldots \cdot a_{ni_n}$.

Faisons correspondre à l'élément (1) la permutation

(2) $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$

de l'ensemble $\{1, \dots, n\}$. Réciproquement: à chaque permutation τ de S_n,

(3) $\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix}$,

correspond un élément unique de l'ensemble $M(A)$, à savoir

(4) $a_{1\tau(1)} \cdot a_{2\tau(2)} \cdot \dots \cdot a_{n\tau(n)}$.

Ainsi, l'application associant à chaque permutation τ de S_n l'élément (4) de l'ensemble $M(A)$ est une *application injective* de l'ensemble S_n sur $M(A)$.

DÉFINITION. On appelle *déterminant de la matrice A* la somme

$$\sum_{\tau \in S_n} \operatorname{sgn}(\tau)\, a_{1\tau(1)} \cdot a_{2\tau(2)} \dots a_{n\tau(n)}.$$

La somme comporte *n!* termes et à chaque permutation τ de S_n dans cette somme correspond exactement un terme.

On notera le déterminant de la matrice A $|A|$ ou det A, ou

$$\begin{vmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \dots & \dots & \dots \\ \alpha_{n1} & \dots & \alpha_{nn} \end{vmatrix}.$$

Si $n = 1$, det $[\alpha_{11}] = \alpha_{11}$. Pour $n = 2$

$$\begin{vmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{vmatrix} = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}.$$

Si $n = 3$, on a

$$\begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{vmatrix} = \alpha_{11}\alpha_{22}\alpha_{33} + \alpha_{13}\alpha_{21}\alpha_{32} + \alpha_{12}\alpha_{23}\alpha_{31} - \\ - \alpha_{13}\alpha_{22}\alpha_{31} - \alpha_{11}\alpha_{23}\alpha_{32} - \alpha_{12}\alpha_{21}\alpha_{33}.$$

PROPOSITION 4.1. *Le déterminant d'une matrice avec ligne (colonne) à éléments nuls est nul.*

Une matrice carrée est dite *diagonale* si sont nuls tous ses éléments ne se trouvant pas sur la diagonale principale.

PROPOSITION 4.2. *Le déterminant d'une matrice diagonale est égal au produit des éléments de sa diagonale principale.*

Une matrice carrée est dite *triangulaire* si sont nuls tous ses éléments se disposant au-dessus (au-dessous) de sa diagonale principale.

PROPOSITION 4.3. *Le déterminant d'une matrice triangulaire est égal au produit des éléments de sa diagonale principale.*

La démonstration des propositions 4.1-4.3 est laissée au soin du lecteur.

Propriétés fondamentales des déterminants. Formulons et démontrons les propriétés rencontrées le plus souvent.

PROPRIÉTÉ 4.1. *Les déterminants d'une matrice carrée A et d'une matrice transposée ${}^tA$ sont égaux.*

Démonstration. Soient $A = \| \alpha_{ik} \|$ une matrice carrée d'ordre n et ${}^tA = \| \beta_{ik} \|$, où $\beta_{ik} = \alpha_{ki}$. On a alors

$$| {}^tA | = \sum_{\tau \in S_n} (\operatorname{sgn} \tau) \beta_{1\tau(1)} \ldots \beta_{n\tau(n)};$$

$$(1) \quad | {}^tA | = \sum_{\tau \in S_n} (\operatorname{sgn} \tau) \alpha_{\tau(1)1} \ldots \alpha_{\tau(n)n}.$$

Etant donné que $\tau = \begin{pmatrix} 1 & \ldots & n \\ \tau(1) & \ldots & \tau(n) \end{pmatrix}$, alors $\tau^{-1} = \begin{pmatrix} \tau(1) & \ldots & \tau(n) \\ 1 & \ldots & n \end{pmatrix}$, ou, si l'on dispose sur la ligne supérieure les nombres dans l'ordre croissant, $\tau^{-1} = \begin{pmatrix} 1 & \ldots & n \\ \tau^{-1}(1) & \ldots & \tau^{-1}(n) \end{pmatrix}$. Dans le produit $\alpha_{\tau(1)1} \ldots \alpha_{\tau(n)n}$ disposons les facteurs de manière que les premiers indices suivent un ordre croissant; il vient alors

$$\alpha_{\tau(1)1} \ldots \alpha_{\tau(n)n} = \alpha_{1\tau^{-1}(1)} \ldots \alpha_{n\tau^{-1}(n)}$$

et l'égalité (1) peut s'écrire sous la forme

$$(2) \quad | {}^tA | = \sum_{\tau^{-1} \in S_n} (\operatorname{sgn} \tau^{-1}) \alpha_{1\tau^{-1}(1)} \ldots \alpha_{n\tau^{-1}(n)}.$$

Vu que la permutation τ^{-1} parcourt une fois tous les éléments de l'ensemble S_n quand τ parcourt tous les éléments de cet ensemble une fois, la somme dans l'égalité (2) est égale au déterminant de la matrice A. Donc, $| {}^tA | = | A |$. □

PROPRIÉTÉ 4.2. *Avec une permutation de deux colonnes (lignes) d'une matrice son déterminant change de signe.*

Démonstration. Soient $A = \| \alpha_{ik} \|$ la matrice $n \times n$ et $B = \| \beta_{ik} \|$ la matrice obtenue à partir de la matrice A par permutation de deux colonnes à indices s et t. Soit σ une transposition de S_n faisant passer s en t, $\sigma = (st)$, il vient alors

$$\beta_{ik} = \alpha_{i\sigma(k)} \quad \text{pour } i, k \in \{1, \ldots, n\},$$

par suite,

$$|B| = \sum_{\tau \in S_n} (\operatorname{sgn} \tau) \beta_{1\tau(1)} \dots \beta_{n\tau(n)} =$$
$$= \sum_{\tau \in S_n} (\operatorname{sgn} \tau) \alpha_{1\sigma\tau(1)} \dots \alpha_{n\sigma\tau(n)}.$$

Selon le théorème 3.4, sgn $(\sigma\tau) = -$ sgn τ. En outre, quand la permutation τ parcourt tous les éléments de l'ensemble S_n une fois, la permutation $\tau' = \sigma\tau$ parcourt également tous les éléments de cet ensemble une fois. On obtient, par conséquent,

$$|B| = -\sum_{\tau' \in S_n} (\operatorname{sgn} \tau') \alpha_{1\tau'(1)} \dots \alpha_{n\tau'(n)} = -|A|,$$

c'est-à-dire $|B| = -|A|$.

PROPRIÉTÉ 4.3. *Le déterminant d'une matrice possédant deux colonnes (lignes) identiques est nul.*

Démonstration. Posons que la matrice $A = \| \alpha_{ik} \|$ possède deux colonnes identiques, par exemple, $A^s = A^t$. Notons σ la transposition (st). Dans ce cas l'égalité $A^s = A^t$ entraîne l'égalité

(1) $\alpha_{1\tau(1)} \dots \alpha_{n\tau(n)} = \alpha_{1\sigma\tau(1)} \dots \alpha_{n\sigma\tau(n)}$.

Faisons correspondre à chaque permutation τ de S_n la permutation $\sigma\tau$. Alors, à la permutation $\sigma\tau$ correspond la permutation τ, car $\sigma(\sigma\tau) = \tau$. Appelons l'ensemble $\{\tau, \sigma\tau\}$ *couple de permutations correspondant entre elles.* L'ensemble S_n se divise en couples de semblables permutations disjoints deux à deux. On est donc en présence d'une partition de l'ensemble S_n:

$$S_n = \bigcup_{\tau \in A_n} \{\tau, \sigma\tau\},$$

où A_n est l'ensemble de toutes les permutations paires de degré n. Donc l'égalité

$$|A| = \sum_{\tau \in S_n} (\operatorname{sgn} \tau) \alpha_{1\tau(1)} \dots \alpha_{n\tau(n)}$$

peut être écrite de la sorte

(2) $$|A| = \sum_{\tau \in A_n} [(\operatorname{sgn} \tau) \alpha_{1\tau(1)} \dots \alpha_{n\tau(n)} + (\operatorname{sgn} \sigma\tau) \alpha_{1\sigma\tau(1)} \dots \alpha_{n\sigma\tau(n)}].$$

De plus, selon le théorème 3.4,

(3) sgn $(\sigma\tau) = -$ sgn τ.

Sur la base de (1) et (3) on conclut que

$$(\operatorname{sgn} \tau) \alpha_{1\tau(1)} \dots \alpha_{n\tau(n)} + (\operatorname{sgn} \sigma\tau) \alpha_{1\sigma\tau(1)} \dots \alpha_{n\sigma\tau(n)} = 0.$$

Ainsi, chaque terme de la somme (2) est nul; par conséquent, $|A| = 0$. □

PROPRIÉTÉ 4.4. *Si tous les éléments d'une ligne (colonne) quelconque de la matrice A sont multipliés par le scalaire λ, le déterminant de la matrice A est alors aussi multiplié par le scalare λ.*

Démonstration. Soient $A = \| \alpha_{ik} \|$ une matrice carrée d'ordre n et B une matrice obtenue à partir de la matrice A après multiplication de la i-ième ligne par le scalaire λ:

$$B = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \cdot & \cdot & \cdot \\ \lambda\alpha_{i1} & \dots & \lambda\alpha_{in} \\ \cdot & \cdot & \cdot \\ \alpha_{n1} & \dots & \alpha_{nn} \end{bmatrix}.$$

On a alors par définition du déterminant

$$|B| = \sum_{\tau \in S_n} (\operatorname{sgn} \tau)\, \alpha_{1\tau(1)} \dots (\lambda\alpha_{i\tau(i)}) \dots \alpha_{n\tau(n)} =$$

$$= \lambda \sum_{\tau \in S_n} (\operatorname{sgn} \tau)\, \alpha_{1\tau(1)} \dots \alpha_{i\tau(i)} \dots \alpha_{n\tau(n)}, \text{ c'est-à-dire } |B| = \lambda |A|.$$

COROLLAIRE 4.4. *Le déterminant d'une matrice dont deux lignes (colonnes) quelconques sont proportionnelles est nul.*

PROPRIÉTÉ 4.5. *Si chaque élément de la i-ième ligne (colonne) d'une matrice carrée A est une somme de m termes, le déterminant de la matrice A est alors égal à la somme de m déterminants, en outre, dans la matrice du premier déterminant dans la i-ième ligne (i-ième colonne) sont contenus les premiers termes de la somme, dans la matrice du deuxième, les seconds termes, etc., tandis que les lignes suivantes sont identiques à celles de la matrice A.*

Démonstration. Supposons que chaque élément de la i-ième ligne de la matrice A est une somme de m termes:

$$(1) \quad \alpha_{ik} = \alpha_{ik}^{(1)} + \dots + \alpha_{ik}^{(m)} \qquad (k = 1, \dots, m).$$

Dans l'égalité

$$|A| = \sum_{\tau \in S_n} (\operatorname{sgn} \tau)\, \alpha_{1\tau(1)} \dots \alpha_{i\tau(i)} \dots \alpha_{n\tau(n)}$$

dans chaque terme de la somme substituons au facteur $\alpha_{i\tau(i)}$ la somme des m termes selon la formule (1) et représentons toute la somme sous forme de m termes:

$$|A| = \sum_{\tau \in S_n} (\operatorname{sgn} \tau)\, \alpha_{1\tau(1)} \dots \alpha_{i\tau(i)}^{(1)} \dots \alpha_{n\tau(n)} + \dots$$

$$\dots + \sum_{\tau \in S_n} (\operatorname{sgn} \tau)\, \alpha_{1\tau(1)} \dots \alpha_{i\tau(i)}^{(m)} \dots \alpha_{n\tau(n)}.$$

En remplaçant chacune des m sommes par le déterminant on aboutit à l'égalité cherchée

$$|A| = \begin{vmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \cdot & \cdot & \cdot \\ \alpha_{i1}^{(1)} & \dots & \alpha_{in}^{(1)} \\ \cdot & \cdot & \cdot \\ \alpha_{n1} & \dots & \alpha_{nn} \end{vmatrix} + \dots + \begin{vmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \cdot & \cdot & \cdot \\ \alpha_{i1}^{(m)} & \dots & \alpha_{in}^{(m)} \\ \cdot & \cdot & \cdot \\ \alpha_{n1} & \dots & \alpha_{nn} \end{vmatrix} . \square$$

PROPRIÉTÉ 4.6. *Si à une colonne (ligne) quelconque de la matrice du déterminant on adjoint une autre colonne (ligne) de la matrice multipliée par un scalaire arbitraire, le déterminant de la matrice ne variera pas.*

Démonstration. Ecrivons la $n \times n$-matrice A sous forme

$$A = (A^1, A^2, \dots, A^n).$$

Admettons que la matrice B s'obtient à partir de la matrice A après adjonction à la première colonne de la k-ième colonne multipliée par le scalaire λ, c'est-à-dire

$$B = (A^1 + \lambda A^k, A^2, \dots, A^n) \quad (k \neq 1).$$

Selon la propriété 4.5, le déterminant de la matrice B peut être représenté sous forme de la somme de deux termes:

$$|B| = |(A^1, A^2, \dots, A^n)| + \lambda |(A^k, A^2, \dots, A^n)|.$$

Dans cette somme le second déterminant est nul comme possédant deux colonnes identiques; donc, $|B| = |A|$. $\square$

COROLLAIRE 4.5. *Si à une colonne (ligne) quelconque de la matrice d'un déterminant on ajoute une combinaison linéaire des autres colonnes (lignes) de la matrice, le déterminant de la matrice ne variera alors pas.*

PROPRIÉTÉ 4.7. *Si une colonne (ligne) quelconque d'une matrice carrée est une combinaison linéaire des autres colonnes (lignes) de la matrice, le déterminant de la matrice est alors nul.*

Cette propriété découle aisément du corollaire 4.5.

Exercices

1. Comment variera le déterminant d'une matrice carrée d'ordre n si chaque élément de la matrice est remplacé par son opposé?
2. Soient A une matrice carrée d'ordre n sur le corps $\mathcal{F}$ et λ un élément de ce corps. Démontrer que $|\lambda A| = \lambda^n |A|$.
3. Comment variera le déterminant d'une matrice carrée d'ordre n à éléments complexes si chaque élément de la matrice est remplacé par son conjugué?
4. Les éléments d'une matrice carrée d'ordre n satisfont à la condition $\alpha_{ik} = \overline{\alpha}_{ki}$, où $\overline{\alpha}_{ki}$ est un nombre complexe conjugué de α_{ik}. Démontrer que $|A|$ est un nombre réel.

5. Démontrer que le déterminant d'une matrice triangulaire est égal au produit des éléments de la diagonale principale de la matrice.

6. Comment variera le déterminant d'une matrice carrée d'ordre n si l'on échange de place la première et la dernière colonnes les autres colonnes étant déplacées vers la gauche en conservant leur disposition?

7. Comment variera le déterminant d'une matrice carrée d'ordre n si les colonnes de la matrice sont écrites dans l'ordre inverse?

8. Supposons que dans le corps $\mathcal{F}$ est satisfaite l'inégalité $1+1 \neq 0$. Démontrer que le déterminant de toute matrice symétrique gauche sur $\mathcal{F}$ d'ordre impair est nul.

9. Démontrer que

$$\begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{vmatrix} = (x_2-x_1)(x_3-x_2)(x_3-x_2).$$

10. Démontrer qu'on a le développement suivant en facteurs linéaires du déterminant de Vandermonde d'ordre n:

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix} = \prod_{n \geqslant i > k \geqslant 1} (x_i - x_k).$$

11. Montrer que si la matrice carrée A est inversible, on a

$|A^{-1}| = |A|^{-1}$.

12. Soit A une matrice carrée. Démontrer que $|A^k| = |A|^k$ pour chaque entier positif k. Montrer que si la matrice A est régulière, on a $|A^k| = |A|^k$ pour tout entier k.

§ 5. Mineurs et compléments algébriques. Théorèmes des déterminants

Mineurs et compléments algébriques. Soient $\mathcal{F}$ un corps de scalaires et $A = \| \alpha_{ik} \| \in F^{m \times n}$;

$$A = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \dots & \dots & \dots \\ \alpha_{m1} & \dots & \alpha_{mn} \end{bmatrix}.$$

Définition. On appelle *sous-matrice de la matrice A* la matrice obtenue à partir de A par suppression d'une collection quelconque de ses lignes et colonnes. La sous-matrice composée de k lignes et k colonnes est appelée *sous-matrice d'ordre k*.

Définition. Le déterminant d'une sous-matrice d'ordre k de la matrice A est appelé *mineur d'ordre k de la matrice A*.

Les mineurs d'ordre 1 de la matrice A sont ses éléments.

Définition. Le déterminant d'une matrice obtenue à partir d'une matrice carrée A en supprimant la i-ième ligne et la k-ième colonne

est appelé *mineur de l'élément* α_{ik} et noté M_{ik}. Le produit $(-1)^{i+k}M_{ik}$ est appelé *complément algébrique* de l'élément α_{ik} et noté A_{ik}.

Remarquons que M_{ik} et $A_{ik} = (-1)^{i+k}M_{ik}$ sont indépendants de l'élément α_{ik}, toutefois, A_{ik} dépend de la parité de la somme $i + k$.

LEMME 5.1. *Soit* $A \in F^{n\times n}$. *Si tous les éléments de la dernière ligne (colonne) de la matrice A sont nuls, excepté, vraisemblablement, l'élément* α_{nn}, *on a alors* $|A| = \alpha_{nn}M_{nn}$.

D é m o n s t r a t i o n. Supposons que

(1) $\alpha_{nk} = 0$ pour $k \in \{1, \ldots, n-1\}$.

Par définition du déterminant,

(2) $$|A| = \sum_{\tau\in S_n} (\operatorname{sgn}\tau)\, \alpha_{1\tau(1)} \ldots \alpha_{n-1\tau(n-1)}\cdot\alpha_{n\tau(n)}.$$

Définissons l'ensemble S'_n par l'égalité

(3) $S'_n = \{\tau \in S_n \mid \tau(n) = n\}$.

Si $\tau \in S_n \setminus S'_n$, alors en vertu de (1) $\alpha_{n\tau(n)} = 0$. Donc, dans la somme (2) tous les termes correspondant aux permutations τ de $S_n\setminus S'_n$ sont nuls. En supprimant dans la somme (2) ces termes, il vient

(4) $$|A| = \alpha_{nn} \sum_{\tau\in S'_n} (\operatorname{sgn}\tau)\, \alpha_{1\tau(1)} \ldots \alpha_{(n-1)\tau(n-1)}.$$

Considérons l'application φ de l'ensemble S'_n sur S_{n-1}:

$$\tau = \begin{pmatrix} 1 & \ldots & (n-1)\,n \\ \tau(1) & \ldots & \tau(n-1)\,n \end{pmatrix} \overset{}{\underset{\varphi}{\mapsto}} \begin{pmatrix} 1 & \ldots & (n-1) \\ \tau(1) & \ldots & \tau(n-1) \end{pmatrix} = \tau'.$$

Ainsi τ' est la restriction de τ à l'ensemble $\{1, \ldots, n-1\}$:

(5) $\tau'(i) = \tau(i)$ pour $i \in \{1, \ldots, n-1\}$,

$$\tau' = \begin{pmatrix} 1 & \ldots & n-1 \\ \tau'(1) & \ldots & \tau'(n-1) \end{pmatrix}.$$

L'application φ est une application injective de l'ensemble S'_n sur S_{n-1}. Comme $\tau(n) = n$ pour $\tau \in S'_n$, le nombre d'inversions dans la permutation τ vaut le nombre d'inversions dans la permutation τ'; par conséquent,

(6) $\operatorname{sgn}\tau' = \operatorname{sgn}\tau$ $(\tau' \in S_{n-1})$.

Sur la base de (5) et (6) on est en mesure d'écrire l'égalité (4) sous forme

$$|A| = \alpha_{nn} \sum_{\tau'\in S_{n-1}} (\operatorname{sgn}\tau')\, \alpha_{1\tau'(1)} \ldots \alpha_{n-1\tau'(n-1)}.$$

Dans cette dernière égalité la somme est le mineur M_{nn} correspondant à l'élément α_{nn}, c'est-à-dire $|A| = \alpha_{nn}\cdot M_{nn}$. □

LEMME 5.2. *Si tous les éléments d'une ligne (colonne) de la matrice carrée A sont nuls, à part, vraisemblablement, un élément, $|A|$ est alors égal au produit de cet élément par son complément algébrique.*

Démonstration. Soit $A = \| \alpha_{ij} \| \in F^{n \times n}$. Supposons que tous les éléments de la i-ième ligne de la matrice A sont nuls excepté, il se peut, l'élément α_{ik}:

(1) $\alpha_{ij} = 0, \ j \in \{1, \ldots, n\} \setminus \{k\}$.

Dans la matrice A on déplacera la i-ième ligne vers le bas jusqu'à ce qu'elle ne devienne la dernière en l'échangeant successivement avec la ligne voisine d'au-dessous. Ensuite, la k-ième colonne de la matrice obtenue sera déplacée vers la droite par permutation avec sa voisine de droite jusqu'à ce qu'elle occupe la dernière place. Finalement la matrice A se transforme en la matrice

$$B = \begin{bmatrix} \alpha_{11} \ldots\ldots\ldots\ldots\ldots \alpha_{1n} & \alpha_{1k} \\ \ldots\ldots\ldots\ldots\ldots\ldots & \\ \alpha_{i-1,1} \ldots\ldots\ldots\ldots & \alpha_{i-1,k} \\ \alpha_{i+1,1} \ldots\ldots\ldots\ldots & \alpha_{i+1,k} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ \alpha_{n1} \ldots\ldots\ldots\ldots\ldots & \alpha_{nk} \\ \alpha_{i1} \ldots \alpha_{i,k-1} \ \alpha_{i,k+1} \ldots \alpha_{in} & \alpha_{ik} \end{bmatrix}.$$

Selon la condition (1), tous les éléments de la dernière ligne de la matrice B sont nuls à part, peut-être, l'élément α_{ik}. Donc, selon le lemme 5.1, on a

(2) $|B| = \alpha_{ik} \cdot M_{ik}$,

où M_{ik} est le mineur de la matrice A correspondant à l'élément α_{ik}. La matrice B a été obtenue à partir de la matrice A par $n - i$ permutations de lignes et $n - k$ permutations de colonnes; donc, selon la propriété 4.3 des déterminants,

$$|B| = (-1)^{n-i+n-k} |A|$$

et

(3) $|A| = (-1)^{i+k} |B|$.

De (2) et (3), on obtient $|A| = (-1)^{i+k} \cdot \alpha_{ik} \cdot M_{ik} = \alpha_{ik} A_{ik}$, c'est-à-dire $|A| = \alpha_{ik} A_{ik}$. □

Développement du déterminant suivant les éléments d'une ligne ou d'une colonne. Lors du calcul des déterminants on se sert souvent du théorème suivant.

THÉORÈME 5.3. *Soit $A \in F^{n \times n}$. Le déterminant de la matrice A est égal à la somme des produits d'éléments d'une colonne (ligne) quelconque*

par leurs compléments algébriques, c'est-à-dire

(1) $|A| = \alpha_{1k}A_{1k} + \ldots + \alpha_{nk}A_{nk}$

$(i, k \in \{1, \ldots, n\})$.

(2) $|A| = \alpha_{i1}A_{i1} + \ldots + \alpha_{in}A_{in}$

Démonstration. Représentons sous forme d'une somme de n colonnes la k-ième colonne A^k de la matrice A :

$$A^k = \begin{bmatrix} \alpha_{1k} \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \alpha_{2k} \\ \vdots \\ 0 \end{bmatrix} + \ldots + \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \alpha_{nk} \end{bmatrix}.$$

Selon la propriété 4.5 des déterminants, à cette représentation correspond la représentation de $|A|$ sous forme d'une somme de n déterminants

$$|A| = \begin{vmatrix} \alpha_{11} & \ldots & \alpha_{1k} & \ldots & \alpha_{1n} \\ \alpha_{21} & \ldots & 0 & \ldots & \alpha_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_{n1} & \ldots & 0 & \ldots & \alpha_{nn} \end{vmatrix} + \ldots + \begin{vmatrix} \alpha_{11} & \ldots & 0 & \ldots & \alpha_{1n} \\ \alpha_{21} & \ldots & 0 & \ldots & \alpha_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_{n1} & \ldots & \alpha_{nk} & \ldots & \alpha_{nn} \end{vmatrix}.$$

Selon le lemme 5.2, le premier terme de cette somme vaut $\alpha_{1k}A_{1k}$, le second, $\alpha_{2k}A_{2k}$, etc. Par conséquent,

$$|A| = \alpha_{1k}A_{1k} + \alpha_{2k}A_{2k} + \ldots + \alpha_{nk}A_{nk}.$$

De façon analogue, on démontre la formule (2). □

La formule (1) porte le nom de *développement du déterminant suivant les éléments de la k-ième colonne*. La formule (2) est le *développement du déterminant suivant les éléments de la i-ième ligne*.

THÉORÈME 5.4. *Soit* $A = \|\alpha_{ij}\| \in F^{n \times n}$. *La somme des produits d'éléments d'une colonne (ligne) quelconque de la matrice A par les compléments algébriques d'éléments correspondants d'une autre colonne (ligne) est nulle, c'est-à-dire*

(3) $\alpha_{1k}A_{1s} + \ldots + \alpha_{nk}A_{ns} = 0 \quad (k \neq s)$,

(4) $\alpha_{i1}A_{m1} + \ldots + \alpha_{in}A_{mn} = 0 \quad (m \neq i)$.

Démonstration. Démontrons la formule (3). Ecrivons A sous forme

$$A = (A^1, \ldots, A^k, \ldots, A^s, \ldots, A^n).$$

En substituant dans la matrice A à la s-ième colonne A^s un vecteur arbitraire $b = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$, on aboutit à la matrice

$$B = (A^1, \ldots, A^k, \ldots, b, \ldots, A^n).$$

Développons $|B|$ suivant les éléments de la s-ième colonne:

$$|B| = \beta_1 A_{1s} + \ldots + \beta_n A_{ns}.$$

Notons que cette égalité se vérifie pour tout jeu des scalaires $\beta_1, \ldots, \beta_n$. En particulier, en y posant $\beta_1 = \alpha_{1k}, \ldots, \beta_n = \alpha_{nk}$, on obtient l'égalité

$$0 = \alpha_{1k} A_{1s} + \ldots + \alpha_{nk} A_{ns} \qquad (k \neq s),$$

car la matrice B aura deux colonnes identiques.

De façon analogue on démontre la formule (4). □

Déterminant d'un produit de matrices. Démontrons d'abord deux lemmes.

LEMME 5.5. *Si E_φ est une matrice élémentaire de même ordre qu'une matrice carrée B, on a alors*

(1) $\quad |E_\varphi B| = |E_\varphi|\,|B| \quad$ et $\quad |E_\varphi| \neq 0.$

D é m o n s t r a t i o n. Toute matrice élémentaire est triangulaire et, partant, son déterminant est égal au produit d'éléments de la diagonale principale. Donc, on a

(2) $$|E_\varphi| = \begin{cases} \lambda & \text{si} \quad E_\varphi = E_{\lambda(i)} \quad (\lambda \neq 0), \\ 1 & \text{si} \quad E_\varphi = E_{(i)+\lambda(k)}; \end{cases}$$

en outre,

(3) $$|E_\varphi B| = \begin{cases} \lambda |B| & \text{si} \quad E_\varphi = E_{\lambda(i)}, \\ |B| & \text{si} \quad E_\varphi = E_{(i)+\lambda(k)}. \end{cases}$$

Sur la base de (2) et (3) on conclut qu'il y a lieu (1). □

LEMME 5.6. *Si $E_1, \ldots, E_s$ sont des matrices élémentaires de même ordre que la matrice carrée B, on a alors*

(4) $\quad |E_1 E_2 \ldots E_s B| = |E_1|\,|E_2| \ldots |E_s|\,|B|.$

D é m o n s t r a t i o n (conduite par récurrence sur le nombre s). Selon le lemme 5.5, le lemme 5.6 se vérifie pour $s = 1$. Supposons que le lemme est vrai pour $s - 1$ facteurs élémentaires et démontrons qu'il se vérifie aussi pour s facteurs. Selon le lemme 5.5, on a

$$|E_1 (E_2 \ldots E_s B)| = |E_1|\,|E_2 \ldots E_s B|.$$

Par hypothèse de récurrence,

$$|E_2 \ldots E_s B| = |E_2|\,|E_3| \ldots |E_s|\,|B|;$$

donc,

$$|E_1 E_2 \ldots E_s B| = |E_1|\,|E_2| \ldots |E_s|\,|B|.$$

L'égalité (4) est ainsi vraie pour tout s. □

COROLLAIRE 5.7. *Si $E_1, \ldots, E_s$ sont des matrices élémentaires d'un même ordre, on a alors*

$$| E_1E_2 \ldots E_s | = | E_1 | | E_2 | \ldots | E_s |.$$

THÉORÈME 5.8. *Le déterminant d'un produit de deux matrices carrées est égal au produit des déterminants de ces matrices*, c'est-à-dire $| AB | = | A | | B |$.

D é m o n s t r a t i o n. Premier cas: les lignes de la matrice A sont linéairement indépendantes. Selon le théorème 2.8, la matrice A peut être représentée sous forme d'un produit de matrices élémentaires $A = E_1, \ldots, E_s$, donc, $AB = E_1 \ldots E_sB$. Selon le lemme 5.6, on a

$$| AB | = | E_1 | \ldots | E_s | | B |.$$

De plus, selon le corollaire 5.7,

$$| A | = | E_1 \ldots E_s | = | E_1 | | E_2 | \ldots | E_s |;$$

par conséquent, $| AB | = | A | | B |$.

Second cas: les lignes de la matrice A sont linéairement dépendantes. Dans ce cas on peut faire passer la matrice A par une série de transformations élémentaires régulières en la forme d'une matrice en escalier qu'on notera C; les lignes de la matrice étant linéairement dépendantes, C comporte donc une ligne à éléments partout nuls. Si

$$A \xrightarrow{\varphi_1 \ldots \varphi_s} C,$$

selon la propriété 2.4 des matrices élémentaires, $E_{\varphi_1} \ldots E_{\varphi_s} \cdot A = C$. Multiplions cette égalité à droite par la matrice B:

$$E_{\varphi_1} \ldots E_{\varphi_s} AB = CB.$$

Selon le lemme 5.6, $| E_{\varphi_1} | \ldots | E_{\varphi_s} | | AB | = | CB |$. Comme C et, partant, CB sont des matrices possédant une ligne à éléments partout nuls, on a $| CB | = 0$. En outre, (selon le lemme 5.5),

$$| E_{\varphi_1} | \neq 0, \ldots, | E_{\varphi_s} | \neq 0, | E_{\varphi_1} | \ldots | E_{\varphi_s} | \neq 0;$$

par conséquent, $| AB | = 0$. Comme les lignes de la matrice A sont linéairement dépendantes, une des lignes de la matrice A est donc une combinaison linéaire des autres lignes. Aussi, (selon la propriété 4.7 des déterminants) a-t-on $| A | = 0$. Par conséquent, $| A | | B | = 0$.

Bref, $| AB | = | A | | B |$. □

Conditions nécessaires et suffisantes de l'égalité à zéro du déterminant. Comme le montrent les deux théorèmes suivants, il existe

diverses conditions mutuellement équivalentes de l'égalité à zéro du déterminant.

THÉORÈME 5.9. *Le déterminant d'une matrice carrée est nul si et seulement si les lignes (colonnes) de la matrice sont linéairement dépendantes.*

D é m o n s t r a t i o n. Soit $A \in F^{n\times n}$. Démontrons que si les lignes de la matrice A sont linéairement indépendantes, alors $|A| \neq 0$. En effet, si les lignes de la matrice A sont linéairement indépendantes, alors selon le théorème 2.8, elle peut être représentée sous forme d'un produit de matrices élémentaires, c'est-à-dire que $A = E_1 \ldots E_s$. Selon le corollaire 5.7, $|A| = |E_1| \ldots |E_s|$. De plus, selon le lemme 5.5, le déterminant d'une matrice élémentaire quelconque est différent de zéro. Donc, $|A| \neq 0$. Selon la loi de contraposition, l'affirmation démontrée est équivalente à l'affirmation: si $|A| = 0$ les lignes de la matrice A sont alors linéairement dépendantes.

Démontrons à présent la réciproque: si les lignes de la matrice carrée A sont linéairement dépendantes, on a alors $|A| = 0$. En effet, si la première ligne A_1 de la matrice A n'a pas d'éléments nuls, une au moins des lignes $A_2, \ldots, A_n$ est alors une combinaison linéaire des autres lignes de la matrice. Donc, selon la propriété 4.7 des déterminants, $|A| = 0$. □

THÉORÈME 5.10. *Pour toute matrice carrée A les quatre affirmations suivantes sont équipotentes:*

(a) $|A| \neq 0$;

(b) *les lignes (colonnes) de la matrice A sont linéairement indépendantes*;

(c) *la matrice A est inversible*;

(d) *la matrice A peut être figurée sous forme d'un produit de matrices élémentaires.*

Ce théorème découle directement des théorèmes 5.9 et 2.8.

Exercices

1. Soient A et C des matrices carrées. Démontrer que

$$\begin{vmatrix} A & 0 \\ B & C \end{vmatrix} = |A| \cdot |C|.$$

2. Démontrer que

$$\begin{vmatrix} a & b & c \\ c & a & b \\ b & c & a \end{vmatrix} = f(\omega_1) f(\omega_2) f(\omega_3),$$

où $f = a + bx + cx^2$ et $\omega_1, \omega_2, \omega_3$ sont les racines cubiques distinctes de l'unité.

3. Calculer le déterminant

$$\begin{vmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{vmatrix}.$$

4. Démontrer que

$$\begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{vmatrix} = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2).$$

5. En se servant uniquement de la définition du déterminant, calculer le déterminant d'une matrice triangulaire A :

$$A = \begin{bmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & 0 & \dots & 0 \\ a_{31} & a_{32} & a_{33} & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix}.$$

6. Combien de sous-matrices carrées d'ordre k possède la matrice $m \times n$?

§ 6. Théorèmes des matrices. Règle de Cramer

Théorème sur le rang d'une matrice. Etudions la liaison du rang de la matrice avec les ordres de ses mineurs non nuls.

THÉORÈME 6.1. *Le rang d'une matrice non nulle est égal au plus grand ordre des mineurs non nuls de la matrice.*

D é m o n s t r a t i o n. Soient A une matrice non nulle et $A \in F^{m \times n}$. Son rang est alors $r = r(A) > 0$. Démontrons que la matrice comporte au moins un mineur non nul d'ordre r. Comme $r = r(A) > 0$, la matrice A possède r lignes linéairement indépendantes. Soit B une sous-matrice de la matrice A composée de r lignes de la matrice A linéairement indépendantes, c'est-à-dire que $B \in F^{r \times n}$, $r(B) = r$. Il s'ensuit de l'égalité $r(B) = r$ que la matrice B possède r colonnes linéairement indépendantes. Soit C une sous-matrice de la matrice B composée de r colonnes linéairement indépendantes de la matrice B, on a alors $C \in F^{r \times r}$, $r(C) = r$. Selon le théorème 5.10, $|C| \neq 0$, car les colonnes de la matrice C sont linéairement indépendantes. Donc, $|C|$ est un mineur non nul d'ordre r de la matrice A.

On vérifie sans peine que pour $k > r(A)$, tout mineur d'ordre k de la matrice A est nul. En effet, pour $k > r(A)$ sont linéairement dépendantes toutes k lignes de la matrice A. Donc les lignes d'une sous-matrice carrée $k \times k$ de la matrice A sont linéairement dépen-

dantes. Par conséquent, selon le théorème 5.9, tout mineur d'ordre k de la matrice A est nul. □

Matrice inverse. Soient $A \in F^{n\times n}$,

$$A=\begin{bmatrix}\alpha_{11} & \alpha_{12} & \dots & \alpha_{1n}\\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n}\\ \cdot & \cdot & \cdot & \cdot\\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn}\end{bmatrix}$$

et A_{ik} le complément algébrique de l'élément α_{ik}.

On appelle *matrice adjointe de* A la matrice

$$A^*=\begin{bmatrix}A_{11} & A_{21} & \dots & A_{n1}\\ A_{12} & A_{22} & \dots & A_{n2}\\ \cdot & \cdot & \cdot & \cdot\\ A_{1n} & A_{2n} & \dots & A_{nn}\end{bmatrix}.$$

En vertu des théorèmes 5.3 et 5.4,

$$A_i(A^*)^k=(\alpha_{i1},\ \dots,\ \alpha_{in})\begin{bmatrix}A_{k1}\\ \vdots\\ A_{kn}\end{bmatrix}=\alpha_{i1}A_{k1}+\dots+\alpha_{in}A_{kn}=$$
$$=\begin{cases}|A| & \text{si } i=k,\\ 0 & \text{si } i\neq k,\end{cases}$$

donc,

$$AA^*=\begin{vmatrix}|A| & 0 & \dots & 0\\ 0 & |A| & \dots & 0\\ \cdot & \cdot & \cdot & \cdot\\ 0 & 0 & \dots & |A|\end{vmatrix}=|A|\,E\ (E \text{ est une matrice unité});$$

(1) $A\,(|A|^{-1}A^*)=E$ si $|A|\neq 0$.

Des calculs analogues conduisent aux égalités

$A^*A=|A|\,E,$

(2) $(|A|^{-1}A^*)\,A=E,$ si $|A|\neq 0.$

Les égalités (1) et (2) montrent que les matrices A et $|A|^{-1}A^*$ sont mutuellement inverses. On a ainsi démontré le théorème suivant.

THÉORÈME 6.2. *Si le déterminant d'une matrice carrée A est différent de zéro, la matrice A est alors inversible et* $A^{-1}=|A|^{-1}A^*$.

Règle de Cramer. Considérons un système de n équations linéaires à n variables

$$(1)\quad \begin{aligned}&\alpha_{11}x_1+\dots+\alpha_{1n}x_n=\beta_1,\\ &\dots\dots\dots\dots\dots\\ &\alpha_{n1}x_1+\dots+\alpha_{nn}x_n=\beta_n\end{aligned}$$

sur le corps $\mathscr{F}$. Notons par A la matrice fondamentale de ce système: $A = \| \alpha_{ik} \|$.

THÉORÈME 6.3. *Si* $|A| \neq 0$ *le système d'équations linéaires* (1) *possède une solution unique qu'exprime les formules*

$$(2) \quad x_1 = |A|^{-1}(\beta_1 A_{11} + \ldots + \beta_n A_{n1}), \ldots$$
$$\ldots, x_n = |A|^{-1}(\beta_1 A_{1n} + \ldots + \beta_n A_{nn}).$$

Démonstration. En posant $\mathscr{X} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, $b = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$, écrivons le système (1) sous forme d'une équation matricielle

$$(3) \quad A\mathscr{X} = b,$$

équipotente au système (1). Selon le théorème 5.9, il s'ensuit de la condition $|A| \neq 0$ que les lignes de la matrice A sont linéairement indépendantes et que les systèmes (3) et (1) admettent une solution unique $\mathscr{X} = A^{-1}b$.

De là, puisque (selon le théorème 6.2) $A^{-1} = |A|^{-1}A^*$, il vient

$$A^{-1}b = |A|^{-1} \begin{bmatrix} A_{11} & \ldots & A_{n1} \\ \cdots & \cdots & \cdots \\ A_{1n} & \ldots & A_{nn} \end{bmatrix} \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} =$$
$$= |A|^{-1} \begin{bmatrix} \beta_1 A_{11} + \ldots + \beta_n A_{n1} \\ \cdots \\ \beta_1 A_{1n} + \ldots + \beta_n A_{nn} \end{bmatrix}$$

et

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} |A|^{-1}(\beta_1 A_{11} + \ldots + \beta_n A_{n1}) \\ \cdots \\ |A|^{-1}(\beta_1 A_{1n} + \ldots + \beta_n A_{nn}) \end{bmatrix}.$$

De cette dernière égalité s'ensuivent les formules (2). □

Les formules (2) sont habituellement appelées *formules de Cramer*, tandis que le théorème 6.3 est nommé *règle de Cramer*.

Notons $A(k)$ la matrice obtenue à partir de la matrice A en substituant à la k-ième colonne la colonne des termes libres du système (1):

$$A(1) = \begin{bmatrix} \beta_1 & \alpha_{12} & \ldots & \alpha_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ \beta_n & \alpha_{n2} & \ldots & \alpha_{nn} \end{bmatrix}, \ldots, A(n) = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n-1} & \beta_1 \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{n1} & \ldots & \alpha_{nn-1} & \beta_n \end{bmatrix}.$$

En développant le déterminant de la matrice $A(k)$ suivant les éléments de la k-ième colonne, on obtient

$$|A(k)| = \beta_1 A_{1k} + \ldots + \beta_n A_{nk} \quad (k = 1, \ldots, n).$$

Ces égalités permettent de reformuler le théorème 6.3 de la façon suivante.

THÉORÈME 6.4. *Si* $|A| \neq 0$ *le système d'équations linéaires* (1) *admet une solution unique explicitée par les formules*

$$(2) \quad x_1 = \frac{|A(1)|}{|A|}, \ldots, x_n = \frac{|A(n)|}{|A|}.$$

Conditions pour lesquelles un système de n équations linéaires homogènes à n variables admet des solutions non nulles.

THÉORÈME 6.5. *Un système de n équations linéaires homogènes à n variables a des solutions non nulles si et seulement si le déterminant de la matrice du système est nul.*

Démonstration. Soit donné un système d'équations linéaires homogènes

$$(1) \quad \begin{aligned} &\alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &\alpha_{n1}x_1 + \ldots + \alpha_{nn}x_n = 0, \end{aligned}$$

$A = \| \alpha_{ik} \|$ étant la matrice de ce système. Le système (1) a des solutions non nulles si et seulement si les colonnes de la matrice A sont linéairement dépendantes. Les colonnes de la matrice A sont linéairement dépendantes si et seulement si $|A| = 0$. Par conséquent, le système (1) admet des solutions non nulles si et seulement si $|A| = 0$. □

COROLLAIRE 6.6. *L'équation matricielle* $A\mathscr{X} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$, *où* $A \in F^{n\times n}$, $\mathscr{X} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ *a des solutions non nulles si et seulement si* $|A| = 0$.

Exercices

1. Montrer que le rang d'un produit de matrices ne dépasse pas celui de chacun des facteurs.
2. Soient A et B des matrices carrées d'ordre n. Montrer que les équations $A\mathscr{X} = B$ et $\mathscr{X}A = B$, où $\mathscr{X}$ est la matrice cherchée, sont insolubles quand le rang de la matrice B dépasse celui de A.
3. Soient A et B des matrices rectangulaires possédant le même nombre de lignes et C la matrice obtenue de la matrice A par adjonction à droite de la matrice B. Démontrer que l'équation matricielle $A\mathscr{X} = B$, où $\mathscr{X}$ est la matrice cherchée, a une solution si et seulement si le rang de la matrice A est égal à celui de la matrice C.

4. Soit $A\mathscr{X} = B$ une équation matricielle, où $\mathscr{X}$ est la matrice cherchée, et $\mathscr{X}_0$ sa solution quelconque. Démontrer que chaque solution de l'équation matricielle peut s'écrire sous la forme $\mathscr{X}_0 + \mathscr{Y}$, où $\mathscr{Y}$ est la solution de l'équation homogène $A\mathscr{Y} = 0$, et réciproquement.

5. Chercher toutes les matrices complexes dont les carrés sont égaux à une matrice nulle.

6. Etudier l'équation $\mathscr{X}A = 0$, où A est la matrice donnée et $\mathscr{X}$ la matrice cherchée de deuxième ordre.

7. Chercher toutes les matrices complexes de deuxième ordre dont les carrés sont égaux à une matrice unité.

8. Soient A et B des matrices $m \times n$. Démontrer que $r(A + B) \leqslant r(A) + r(B)$ *).

9. Soient A et B des matrices possédant un même nombre de lignes et C une matrice obtenue en adjoignant à A toutes les colonnes de la matrice B. Démontrer que $r(C) \leqslant r(A) + r(B)$.

10. Montrer que si le produit AB est une matrice régulière, alors les matrices A et B sont également régulières.

11. Soit A une matrice carrée régulière d'ordre n. Montrer que pour toute matrice carrée B d'ordre n, les matrices AB, B et BA ont même rang.

12. Soient A, B des matrices $n \times n$ de rang r et s respectivement. Démontrer que $r(AB) \geqslant r + s - n$.

13. Démontrer que la matrice $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ est inversible si et seulement si $ad - bc \neq 0$.

14. Démontrer que si la matrice $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ est inversible, alors $A^{-1} = (ad - bc)^{-1} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

15. Démontrer que chaque matrice triangulaire A (sur le corps $\mathscr{F}$) aux éléments non nuls sur la diagonale principale est inversible et la matrice A^{-1} est une matrice triangulaire.

16. Soient A, B des matrices $n \times n$ régulières sur le corps $\mathscr{F}$. Montrer que les égalités $AB = BA$, $AB^{-1} = B^{-1}A$, $A^{-1}B = BA^{-1}$, $A^{-1}B^{-1} = B^{-1}A^{-1}$ sont équipotentes entre elles.

17. Soit A une matrice $m \times n$ sur le corps $\mathscr{F}$. Démontrer que:

(a) il existe une matrice $n \times m$ $\mathscr{X}$, telle que $\mathscr{X}A = E$, où E est une matrice unité $n \times n$ si et seulement si le rang de A vaut n;

(b) il existe une matrice $n \times m$ telle que $A\mathscr{Y} = E$, où E est une matrice $m \times m$ unité si et seulement si le rang de A vaut m.

18. Soit A une matrice triangulaire $n \times n$ (sur le corps $\mathscr{F}$) dont tous les éléments de la diagonale principale valent 1. Supposons que $B = A - E$, où E est une matrice unité $n \times n$. Démontrer que:

(a) $B^{n+1} = 0$;

(b) la matrice A est inversible et $A^{-1} = (E + B)^{-1} = E - B + B^2 - \ldots + (-1)^n B^n$;

(c) $(E - B)^{-1} = E + B + B^2 + \ldots + B^n$.

19. Soit A une matrice triangulaire (sur un corps) à éléments non nuls sur la diagonale principale. Démontrer que la matrice A est inversible.

20. Chercher les conditions que doit satisfaire une matrice carrée à éléments entiers pour que tous les éléments de la matrice inverse soient des entiers.

21. Soient A une matrice $n \times n$ carrée et A^* la matrice adjointe à A. Démontrer que:

(a) si A est une matrice singulière, alors la matrice AA^* est nulle;

*) $r(A)$ est ici le rang de la matrice A.

(b) $A^* = |A| A^{-1}$ si A est une matrice inversible;

(c) A^* est une matrice singulière si et seulement si la matrice A est singulière;

(d) $|A^*| = |A|^{n-1}$;

(e) si la matrice A est symétrique ou symétrique gauche, alors A^* est aussi symétrique ou symétrique gauche;

(f) si A est une matrice triangulaire, alors A^* est aussi triangulaire.

22. Soit A^* une matrice triangulaire adjointe à la matrice $n \times n$ A. Démontrer que:

(a) si le rang $A < n - 1$, alors A^* est une matrice nulle;

(b) si A est de rang $n - 1$, alors le rang de A^* est 1;

(c) si A a le rang n, le rang de A^* est alors aussi n.

23. Soit A une matrice triangulaire $n \times n$ sur le corps $\mathcal{F}$. Démontrer que la matrice A est inversible si et seulement si tous les éléments de la matrice A se rangeant sur la diagonale principale sont différents de zéro.

15—01762

CHAPITRE VII

ESPACES VECTORIELS

§ 1. Espaces vectoriels

Notion d'espace vectoriel. Soient $\mathcal{F}$ un corps et F son ensemble de base. Les éléments de l'ensemble F seront appelés *scalaires*, tandis que $\mathcal{F}$ sera nommé *corps des scalaires*.

Soient V un ensemble non vide et $F \times V$ le produit direct des ensembles F et V. Soit donnée l'application

$$\omega: F \times V \to V$$

associant à chaque couple $\langle \lambda, a \rangle$ de $F \times V$ un élément unique de l'ensemble V noté λa et appelé *produit duscalaire* λ *et de l'élément* a. Si le scalaire λ est fixé, l'application ω induit l'application

$$\omega_\lambda: \{\lambda\} \times V \to V,$$

qui est la restriction ω à l'ensemble $\{\lambda\} \times V$. L'application ω_λ avec λ fixé peut être aussi assimilée à une opération à une place (singulaire) $V \to V$ associant à chaque élément a de V un élément λa de V. Ainsi, $\omega_\lambda a = \lambda a$ pour tout a de V.

Exemple. Soient $\mathcal{F}$ un corps, $V = F^n$ et λ un élément fixé de F. Notons ω_λ l'application V dans V associant à chaque vecteur $(\alpha_1, \ldots, \alpha_n)$ de F^n le vecteur $(\lambda\alpha_1, \ldots, \lambda\alpha_n)$ de F^n appelé *produit du scalaire* λ *et du vecteur arithmétique* $(\alpha_1, \ldots, \alpha_n)$.

Définition. L'ensemble V avec l'opération binaire donnée sur lui $+$ (appelée addition) et l'opération de multiplication des éléments du corps des scalaires $\mathcal{F}$ par les éléments de l'ensemble V est appelé *espace vectoriel sur le corps* $\mathcal{F}$ si pour tous $\mathbf{a}$, $\mathbf{b}$ de V et α, β de F sont satisfaites les conditions (axiomes) suivantes:

(1) l'algèbre $\langle V, +, - \rangle$, où $-$ est l'opération de multiplication par le scalaire (-1) des éléments de V, est un groupe abélien;

(2) $(\alpha\beta)\,\mathbf{a} = \alpha\,(\beta\mathbf{a})$;

(3) $\alpha\,(\mathbf{a} + \mathbf{b}) = \alpha\mathbf{a} + \alpha\mathbf{b}$;

(4) $(\alpha + \beta)\,\mathbf{a} = \alpha\mathbf{a} + \beta\mathbf{a}$;

(5) $1 \cdot \mathbf{a} = \mathbf{a}$.

L'espace vectoriel muni de l'ensemble de base V est noté $\mathscr{V}$. Ainsi, l'espace vectoriel $\mathscr{V}$ est une algèbre munie de l'ensemble de base V, dans lequel l'opération binaire $+$ et les opérations singulaires ω_λ (multiplication par le scalaire λ de F) sont des opérations principales, c'est-à-dire que

$$\mathscr{V} = \langle V, +, \{\omega_\lambda \mid \lambda \in F\}\rangle,$$

les opérations principales satisfaisant aux conditions (1)-(5) appelées *axiomes de l'espace vectoriel.*

Le groupe $\langle V, +, -\rangle$ est dit *groupe additif de l'espace vectoriel* $\mathscr{V}$. Le zéro $\mathbf{0}$ de ce groupe est appelé *vecteur nul de l'espace vectoriel* $\mathscr{V}$. Les éléments de l'ensemble V sont appelés *vecteurs de l'espace vectoriel* $\mathscr{V}$. Les vecteurs $\mathbf{a}$ et $(-1)\,\mathbf{a}$ sont dits *opposés l'un à l'autre.*

Exemples d'espaces vectoriels. 1. Soit $\mathscr{F}^n$ un espace arithmétique à n dimensions sur le corps $\mathscr{F}$; $\mathscr{F}^n$ est un espace vectoriel sur le corps $\mathscr{F}$. Cas particuliers importants : $\mathscr{Q}^m$, $\mathscr{R}^n$, $\mathscr{C}^n$.

2. L'ensemble de tous les vecteurs du plan est un espace vectoriel sur le corps $\mathscr{R}$ des nombres réels par rapport aux opérations d'addition et de multiplication par des nombres réels.

3. Soit $F^{m\times n}$ un ensemble de toutes les matrices $m \times n$ sur le corps $\mathscr{F}$. L'algèbre $\langle F^{m\times n}, +, \{\omega_\lambda \mid \lambda \in F\}\rangle$, où $+$ est l'opération d'addition des matrices et ω_λ l'opération de multiplication des matrices par le scalaire λ, est un espace vectoriel sur le corps $\mathscr{F}$. On l'appelle *espace vectoriel des matrices* $m \times n$ sur le corps $\mathscr{F}$.

4. L'ensemble de toutes les applications de l'ensemble $\mathbf{R}$ dans $\mathbf{R}$ est un espace vectoriel sur le corps $\mathscr{R}$ par rapport aux opérations d'addition des applications et de multiplication des applications par des nombres réels.

5. L'ensemble $\mathbf{C}$ de tous les nombres complexes est un espace vectoriel sur le corps $\mathscr{R}$ par rapport aux opérations d'addition des nombres complexes et de multiplication par des nombres réels.

Propriétés élémentaires des espaces vectoriels.

THÉORÈME 7.1. *Soient $\mathscr{V}$ un espace vectoriel sur le corps $\mathscr{F}$,* $\mathbf{a}, \mathbf{b} \in V$ *et* $\alpha, \beta \in F$. *Alors,*

(1) *si* $\mathbf{a} + \mathbf{b} = \mathbf{a}$, *on a* $\mathbf{b} = \mathbf{0}$;

(2) $0 \cdot \mathbf{a} = \mathbf{0}$;

(3) $\alpha \cdot \mathbf{0} = \mathbf{0}$;

(4) *si* $\mathbf{a} + \mathbf{b} = \mathbf{0}$, *on a* $\mathbf{b} = (-1)\,\mathbf{a} = -\mathbf{a}$;

(5) *si* $\alpha \cdot \mathbf{a} = \alpha \cdot \mathbf{b}$ *et* $\alpha \neq 0$, *on a* $\mathbf{a} = \mathbf{b}$;

(6) *si* $\alpha \cdot \mathbf{a} = \mathbf{0}$, *on a* $\alpha = 0$ *ou* $\mathbf{a} = \mathbf{0}$;

(7) *si* $\alpha \mathbf{a} = \beta \mathbf{a}$ *et* $\mathbf{a} \neq \mathbf{0}$, *on a* $\alpha = \beta$.

Démonstration. (1) Vu que $\mathbf{0}$ est un zéro du groupe additif de l'espace $\mathscr{V}$, on a $\mathbf{a} + \mathbf{0} = \mathbf{a}$. Aussi, peut-on écrire l'égalité

$\mathbf{a} + \mathbf{b} = \mathbf{a}$ sous forme $\mathbf{a} + \mathbf{b} = \mathbf{a} + \mathbf{0}$. Selon la loi de simplification (concernant les groupes) il s'ensuit que $\mathbf{b} = \mathbf{0}$.

(2) Selon l'axiome (4) de l'espace vectoriel, il vient

$$0 \cdot \mathbf{a} + 0 \cdot \mathbf{a} = (0 + 0)\, \mathbf{a} = 0 \cdot \mathbf{a}, \text{ c'est-à-dire } 0 \cdot \mathbf{a} + 0 \cdot \mathbf{a} = 0 \cdot \mathbf{a}.$$

Selon la propriété (1), il s'ensuit que $0 \cdot \mathbf{a} = \mathbf{0}$.

(3) Selon l'axiome (3) de l'espace vectoriel,

$$\alpha \cdot \mathbf{0} + \alpha \cdot \mathbf{0} = \alpha\, (\mathbf{0} + \mathbf{0}) = \alpha \cdot \mathbf{0}, \text{ c'est-à-dire } \alpha \cdot \mathbf{0} + \alpha \cdot \mathbf{0} = \alpha \cdot \mathbf{0}.$$

De la propriété (1), il se dégage l'égalité $\alpha \cdot \mathbf{0} = \mathbf{0}$.

(4) Vu que $\mathbf{a} + (-1)\, \mathbf{a} = \mathbf{0}$, l'égalité $\mathbf{a} + \mathbf{b} = \mathbf{0}$ peut être écrite sous forme $\mathbf{a} + \mathbf{b} = \mathbf{a} + (-1)\, \mathbf{a}$. Selon la loi de simplification (concernant les groupes), il s'ensuit que $\mathbf{b} = (-1) \cdot \mathbf{a}$.

(5) Pour $\alpha \neq 0$ de $\alpha\mathbf{a} = \alpha\mathbf{b}$, il s'ensuit que $\alpha^{-1}\, (\alpha\mathbf{a}) = \alpha^{-1}\, (\alpha\mathbf{b})$ et, en vertu de l'axiome (2) $\mathbf{a} = \mathbf{b}$.

(6) Comme $\alpha\mathbf{0} = \mathbf{0}$, on peut écrire l'égalité $\alpha\mathbf{a} = \mathbf{0}$ sous forme $\alpha\mathbf{a} = \alpha \cdot \mathbf{0}$. Pour $\alpha \neq 0$, selon la propriété (5), on en tire que $\mathbf{a} = \mathbf{0}$.

(7) En ajoutant $(-\beta\mathbf{a})$ aux deux membres de l'égalité $\alpha\mathbf{a} = \beta\mathbf{a}$, on obtient $\alpha\mathbf{a} + (-\beta)\, \mathbf{a} = \mathbf{0}$, $(\alpha - \beta)\, \mathbf{a} = \mathbf{0}$. Pour $\mathbf{a} \neq 0$, selon la propriété (6), il s'ensuit que $\alpha - \beta = 0$ et $\alpha = \beta$.

Dépendance et indépendance linéaires d'un système de vecteurs. Soit $\mathscr{V}$ un espace vectoriel sur le corps $\mathscr{F}$. On dit que le système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ de l'espace est *linéairement dépendant* s'il existe des scalaires $\lambda_1, \ldots, \lambda_m \in F$ non tous nuls tels que $\lambda_1\mathbf{a}_1 + \ldots$ $\ldots + \lambda_m\mathbf{a}_m = \mathbf{0}$.

Le système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ de l'espace $\mathscr{V}$ est dit *linéairement indépendant* si pour tous scalaires $\lambda_1, \ldots, \lambda_m \in F$ de l'égalité $\lambda_1\mathbf{a}_1 + \ldots + \lambda_m\mathbf{a}_m = \mathbf{0}$ s'ensuivent les égalités $\lambda_1 =$ $= 0, \ldots, \lambda_m = 0$.

Pour des espaces vectoriels arbitraires restent vrais: les énoncés et les démonstrations des propriétés et des théorèmes du § 5.1 sur les dépendance et indépendance linéaires des systèmes (propriétés 5.1.1-5.1.5, théorèmes et corollaires 5.1.2-5.1.5); les définitions et théorèmes du § 5.1 sur les systèmes équivalents de vecteurs et leurs démonstrations (théorèmes 5.1.6-5.1.8); les théorèmes et propositions (et leurs démonstrations) du § 5.1 sur la base et le rang d'un système fini de vecteurs (théorèmes 5.1.9, théorèmes et propositions 5.1.10-5.1.15).

Exercices

1. Soit $\mathscr{F} = \mathscr{Z}_2$ un corps des classes résiduelles modulo 2. Combien de vecteurs contient l'espace vectoriel $\mathscr{V} = \mathscr{F}^n$, espace arithmétique à n dimensions sur le corps $\mathscr{F}$?

2. Soient $\mathscr{F}$ un corps des scalaires et $F^{2\times 2}$ l'ensemble de toutes les matrices 2×2 sur le corps $\mathscr{F}$. Montrer que l'algèbre

$$\langle F^{2\times 2}, +, -, \{\omega_\lambda \mid \lambda \in F\}\rangle,$$

où $+$ est l'opération d'addition des matrices et ω_λ l'opération de multiplication par le scalaire λ, est un espace vectoriel sur le corps $\mathcal{F}$.

3. Soit $\mathbf{C}^{\mathbf{R}}$ l'ensemble de toutes les applications de l'ensemble $\mathbf{R}$ des nombres réels dans l'ensemble $\mathbf{C}$ de nombres complexes. Montrer que l'algèbre

$$\langle \mathbf{C}^{\mathbf{R}}, +, -, \{\omega_\lambda \mid \lambda \in \mathbf{C}\}\rangle,$$

où $+$ est l'opération d'addition des fonctions, ω_λ l'opération de multiplication par le scalaire λ, $((\lambda f)(x) = \lambda f(x), \lambda \in \mathbf{C})$ et $-f = (-1)\cdot f$, est un espace vectoriel sur le corps des nombres complexes.

4. Soit $\mathbf{R}^{\mathbf{C}}$ l'ensemble de toutes les applications de l'ensemble $\mathbf{C}$ des nombres complexes dans l'ensemble $\mathbf{R}$ des nombres réels. Montrer que l'algèbre

$$\langle \mathbf{R}^{\mathbf{C}}, +, -, \{\omega_\lambda \mid \lambda \in \mathbf{R}\}\rangle,$$

où $+$ est l'opération d'addition des fonctions et ω_λ l'opération de multiplication par le scalaire λ, est un espace vectoriel sur le corps $\mathcal{R}$ des nombres réels.

5. Soient $\mathcal{R}$ un corps des nombres réels et $\mathcal{Q}$ un corps des nombres rationnels. Montrer que l'algèbre

$$\langle \mathbf{R}, +, -, \{\omega_\lambda \mid \lambda \in Q\}\rangle,$$

où $+$ est une opération banale d'addition des nombres réels et ω_λ une opération banale de multiplication par un nombre rationnel λ, est un espace vectoriel sur le corps $\mathcal{Q}$.

6. Soient $\mathbf{C}$ l'ensemble de tous les nombres complexes et $\mathbf{Q}$ l'ensemble de tous les nombres rationnels. Montrer que l'algèbre

$$\langle \mathbf{C}, +, -, \{\omega_\lambda \mid \lambda \in Q\}\rangle,$$

où $+$ est une addition banale des nombres complexes et ω_λ une opération de multiplication par le scalaire λ (par le nombre rationnel λ), est un espace vectoriel sur le corps $\mathcal{Q}$.

7. Soit V l'ensemble de toutes les fonctions réelles doublement dérivables $f: \mathbf{R} \to \mathbf{R}$, satisfaisant à l'équation différentielle $f'' + f = 0$. Montrer que l'algèbre

$$\langle V, +, -, \{\omega_\lambda \mid \lambda \in \mathbf{R}\}\rangle,$$

où $+$ est une opération d'addition et ω_λ une opération de multiplication de la fonction par un scalaire (un nombre réel), est un espace vectoriel sur le corps $\mathcal{R}$.

8. Soit V l'ensemble de toutes les fonctions réelles n fois dérivables $f: \mathbf{R} \to \mathbf{R}$, satisfaisant à la condition (à l'équation différentielle)

$$f^{(n)} + \lambda_{n-1} f^{(n-1)} + \ldots + \lambda_1 f' + \lambda_0 f = 0,$$

où $f^{(k)}$ est la k-ième dérivée de la fonction f et $\lambda_0, \ldots, \lambda_{n-1} \in \mathbf{R}$. Démontrer que l'algèbre $\langle V, +, -, \{\omega_\lambda \mid \lambda \in \mathbf{R}\}\rangle$, où $+$ est une opération d'addition des fonctions et ω_λ une opération de multiplication par le scalaire λ, est un espace vectoriel sur le corps $\mathcal{R}$.

9. Montrer que le système composé d'un seul vecteur est linéairement indépendant si et seulement si le vecteur n'est pas nul.

10. Démontrer qu'un système de deux vecteurs est linéairement dépendant si et seulement si l'un des vecteurs est déduit de l'autre par multiplication par un scalaire.

11. Montrer que les vecteurs (α, β), (γ, δ) d'un espace vectoriel arithmétique à deux dimensions sont linéairement dépendants si et seulement si $\alpha\delta - \beta\gamma = 0$.

12. A quelles conditions doivent satisfaire les scalaires α, β, γ pour que le système des vecteurs $(1, \alpha, \alpha^2)$, $(1, \beta, \beta^2)$, $(1, \gamma, \gamma^2)$ d'un espace vectoriel

arithmétique à trois dimensions sur le corps numérique $\mathcal{F}$ soit linéairement indépendant?

13. Soit $\mathcal{V}$ un espace vectoriel sur le corps numérique $\mathcal{F}$. Montrer que si les vecteurs **a**, **b**, **c** de l'espace $\mathcal{V}$ sont linéairement indépendants, alors les vecteurs $\mathbf{a}+\mathbf{b}$, $\mathbf{a}+\mathbf{c}$, $\mathbf{b}+\mathbf{c}$ sont aussi linéairement indépendants. Est-ce vrai au cas où le corps des scalaires $\mathcal{F}$ comporte deux éléments?

14. Soit $\mathcal{V}=\mathcal{F}^n$ un espace arithmétique à n dimensions sur le corps $\mathcal{F}$. Montrer que le système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ de l'espace $\mathcal{V}$ est linéairement indépendant si et seulement si le rang de la matrice $m \times n$ aux lignes $\mathbf{a}_1, \ldots, \mathbf{a}_m$ vaut m.

15. Montrer qu'un système des vecteurs non nuls $\mathbf{a}_1, \ldots, \mathbf{a}_m$ de l'espace vectoriel $\mathcal{V}$ est linéairement indépendant si et seulement si $a_k \notin L(\mathbf{a}_1, \ldots, \mathbf{a}_{k-1})$ pour tous $k = 2, 3, \ldots, m$.

16. Soient $\mathcal{F}$ un corps fini composé de p éléments et $\mathcal{V}=\mathcal{F}^n$. Combien y a-t-il de systèmes distincts linéairement indépendants comportant k vecteurs $(k<n)$ dans l'espace $\mathcal{V}$?

17. Soient $\mathcal{F}$ un corps et A la matrice $n \times n$ sur $\mathcal{F}$. Démontrer que pour un m suffisamment grand le système des matrices $E, A, A^2, \ldots, A^m$, où E est une matrice unité $n \times n$, est linéairement dépendant sur le corps $\mathcal{F}$.

18. Soit $\mathbf{a}_1, \ldots, \mathbf{a}_m \in Q$. Démontrer que le système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ est linéairement indépendant dans l'espace $\mathcal{R}^n$ si et seulement s'il est linéairement indépendant dans l'espace $\mathcal{Q}^n$.

19. Soit $\mathcal{F}$ un corps fini composé de p éléments. Combien de sous-espaces distincts à k dimensions $(k<n)$ possède l'espace vectoriel $\mathcal{F}^n$?

§ 2. Sous-espaces d'un espace vectoriel

Sous-espace vectoriel. Soient $\mathcal{V}$ un espace vectoriel sur le corps $\mathcal{F}$ et $U \subset V$. L'ensemble U est dit *fermé* dans $\mathcal{V}$ s'il est fermé relativement aux opérations principales de $\mathcal{V}$, opérations d'addition et de multiplication par un scalaire, c'est-à-dire que pour tous **a**, **b** de U et λ quelconque de F, on a $\mathbf{a}+\mathbf{b} \in U$ et $\lambda\mathbf{a} \in U$.

Définition. On appelle *sous-espace d'un espace vectoriel* $\mathcal{V}$ toute sous-algèbre de l'espace $\mathcal{V}$ considéré comme une algèbre.

Soit $\mathcal{V} = \langle V, +, \{\omega_\lambda \mid \lambda \in F\}\rangle$ un espace vectoriel sur $\mathcal{F}$. Soient $\mathcal{U}$ une sous-algèbre de l'espace $\mathcal{V}$ et U son ensemble de base. Alors U est un sous-ensemble non vide de l'ensemble V fermé dans $\mathcal{V}$. Soient $\oplus$ et ω'_λ les restrictions des opérations principales « + » et ω_λ de l'espace $\mathcal{V}$ à l'ensemble U, c'est-à-dire

$$\mathbf{a} \oplus \mathbf{b} = \mathbf{a}+\mathbf{b} \text{ pour tous } \mathbf{a}, \mathbf{b} \text{ de } U,$$

$$\omega'_\lambda\mathbf{a} = \omega_\lambda\mathbf{a} = \lambda\mathbf{a} \text{ pour tout } \mathbf{a} \text{ de } U;$$

alors,

$$(1) \quad \mathcal{U} = \langle U, \oplus, \{\omega'_\lambda \mid \lambda \in F\}\rangle.$$

Toutefois, au lieu de la notation (1), on écrit

$$\mathcal{U} = \langle U, +, \{\omega_\lambda \mid \lambda \in F\}\rangle.$$

Indiquons les propriétés suivantes d'un sous-espace.

Propriété 2.1. *Si $\mathcal{V}$ est un espace vectoriel sur le corps $\mathcal{F}$, alors, tout son sous-espace constitue un espace vectoriel sur le corps $\mathcal{F}$.*

PROPRIÉTÉ 2.2. *Si $\mathscr{W}$ est un sous-espace de l'espace vectoriel $\mathscr{U}$ et $\mathscr{U}$ un sous-espace de l'espace vectoriel $\mathscr{V}$, alors $\mathscr{W}$ est un sous-espace de l'espace $\mathscr{V}$.*

On appelle *intersection des sous-espaces* $\mathscr{U}_1, \ldots, \mathscr{U}_m$ de l'espace vectoriel $\mathscr{V}$ le sous-espace $\mathscr{V}$ muni de l'ensemble de base $U_1 \cap U_2 \cap \cap, \ldots, \cap U_m$. On définit de façon analogue l'intersection d'un ensemble infini de sous-espaces de l'espace $\mathscr{V}$.

PROPRIÉTÉ 2.3. *Une intersection de tout ensemble de sous-espaces de l'espace vectoriel $\mathscr{V}$ est un sous-espace de l'espace $\mathscr{V}$.*

Les propriétés 2.2 et 2.3 découlent des théorèmes 3.1.7 et 3.1.9 respectivement.

Enveloppe linéaire d'un ensemble des vecteurs. Soit $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ un ensemble fini des vecteurs de l'espace vectoriel $\mathscr{V}$. Le vecteur $\lambda_1\mathbf{a}_1 + \ldots + \lambda_n\mathbf{a}_n$ est appelé *combinaison linéaire des vecteurs* $\mathbf{a}_1, \ldots, \mathbf{a}_n$ à coefficients dans F.

DÉFINITION. L'ensemble $\{\lambda_1\mathbf{a}_1 + \ldots + \lambda_n\mathbf{a}_n \mid \lambda_1, \ldots, \lambda_n \in F\}$ de toutes les combinaisons linéaires des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_n$ à coefficients dans F est appelé *enveloppe linéaire des vecteurs* $\mathbf{a}_1, \ldots \ldots, \mathbf{a}_n$ et noté $L(\mathbf{a}_1, \ldots, \mathbf{a}_n)$.

On constate sans peine que l'enveloppe linéaire des vecteurs est fermée dans $\mathscr{V}$, c'est-à-dire est fermée relativement à toutes les opérations principales de l'espace $\mathscr{V}$ (addition et multiplication par des scalaires).

DÉFINITION. Le sous-espace de l'espace vectoriel $\mathscr{V}$ avec l'ensemble de base $L(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ est noté $\mathscr{L}(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ et est appelé *sous-espace* étalé sur les vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_n$ ou sous-espace engendré par les vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_n$.

DÉFINITION. On appelle *enveloppe linéaire de l'ensemble M*, $M \subset V$ la collection $L(M)$ de toutes les combinaisons linéaires de vecteurs de M avec coefficients dans F. On appelle *enveloppe linéaire d'un ensemble vide* l'ensemble $\{\mathbf{0}\}$.

L'enveloppe linéaire de l'ensemble M est fermée dans $\mathscr{V}$.

DÉFINITION. Un sous-espace de l'espace $\mathscr{V}$ avec ensemble de base $L(M)$ est noté $\mathscr{L}(M)$ et appelé *sous-espace étalé sur l'ensemble M* ou *sous-espace engendré par l'ensemble M*.

Somme de sous-espaces. Soient $\mathscr{U}_1, \ldots, \mathscr{U}_m$ des sous-espaces de l'espace vectoriel $\mathscr{V}$ et $U_1, \ldots, U_m$ leurs ensembles de base. L'ensemble

$$\{\mathbf{a}_1 + \ldots + \mathbf{a}_m \mid \mathbf{a}_1 \in U_1, \ldots, \mathbf{a}_m \in U_m\}$$

est noté $U_1 + \ldots + U_m$. On vérifie sans peine que cet ensemble est fermé dans l'espace $\mathscr{V}$.

DÉFINITION. Un sous-espace de l'espace $\mathscr{V}$ avec ensemble de base $U_1 + \ldots + U_m$ est appelé *somme des sous-espaces* $\mathscr{U}_1, \ldots, \mathscr{U}_m$ et noté $\mathscr{U}_1 + \ldots + \mathscr{U}_m$.

Notons les propriétés suivantes d'une somme de sous-espaces qui se déduisent sans peine de sa définition.

PROPRIÉTÉ 2.4. Si $\mathcal{L}$ et $\mathcal{U}$ sont des sous-espaces de l'espace vectoriel $\mathcal{V}$, alors $\mathcal{U} + \mathcal{L} = \mathcal{L} + \mathcal{U}$.

PROPRIÉTÉ 2.5. Si $\mathcal{L}, \mathcal{U}, \mathcal{W}$ sont des sous-espaces de l'espace vectoriel $\mathcal{V}$, alors $\mathcal{L} + (\mathcal{U} + \mathcal{W}) = (\mathcal{L} + \mathcal{U}) + \mathcal{W}$.

PROPRIÉTÉ 2.6. Si $\mathcal{L}$ est un sous-espace de l'espace $\mathcal{U}$, alors $\mathcal{L} + \mathcal{U} = \mathcal{U}$.

Soient $\mathcal{L}_1, \ldots, \mathcal{L}_m$ des sous-espaces de l'espace vectoriel $\mathcal{V}$.

DÉFINITION. La somme $\mathcal{L}_1 + \ldots + \mathcal{L}_m$ est appelée *somme directe des sous-espaces* $\mathcal{L}_1, \ldots, \mathcal{L}_m$ et se note $\mathcal{L}_1 \oplus \ldots \oplus \mathcal{L}_m$ si tout vecteur $\mathbf{a}$ de $L_1 + \ldots + L_m$ se représente de façon unique sous forme

$$\mathbf{a} = \mathbf{a}_1 + \ldots + \mathbf{a}_m, \text{ où } \mathbf{a}_1 \in L_1, \ldots, \mathbf{a}_m \in L_m.$$

En d'autres termes, la somme $\mathcal{L}_1 + \ldots + \mathcal{L}_m$ est dite *directe* si l'égalité $\mathbf{a}_1 + \ldots + \mathbf{a}_m = \mathbf{b}_1 + \ldots + \mathbf{b}_m$ entraîne les égalités $\mathbf{a}_1 = \mathbf{b}_1, \ldots, \mathbf{a}_m = \mathbf{b}_m$ pour tous $\mathbf{a}_1, \mathbf{b}_1$ de $L_1, \ldots, \mathbf{a}_m, \mathbf{b}_m$ de L_m.

THÉORÈME 2.1. *La somme des sous-espaces $\mathcal{L}$ et $\mathcal{U}$ de l'espace vectoriel est directe si et seulement si $L \cap U = \{0\}$.*

Démonstration. Posons que $\mathcal{L} + \mathcal{U} = \mathcal{L} \oplus \mathcal{U}$. Alors, pour tout élément $\mathbf{c}$ de $L \cap U$ se vérifie l'égalité $\mathbf{c} + \mathbf{0} = \mathbf{0} + \mathbf{c}$, de laquelle se déduit l'égalité $\mathbf{c} = \mathbf{0}$, car la somme $\mathcal{L} + \mathcal{U}$ est directe. Donc, $L \cap U = \{\mathbf{0}\}$.

Supposons maintenant que $L \cap U = \{\mathbf{0}\}$. Pour tous vecteurs $\mathbf{a}_1, \mathbf{b}_1$ de L et $\mathbf{a}_2, \mathbf{b}_2$ de U l'égalité $\mathbf{a}_1 + \mathbf{a}_2 = \mathbf{b}_1 + \mathbf{b}_2$ entraîne les relations $\mathbf{a}_1 - \mathbf{b}_1 = \mathbf{a}_2 - \mathbf{b}_2 \in L \cap U = \{\mathbf{0}\}$, par suite, $\mathbf{a}_1 = \mathbf{b}_1$ et $\mathbf{a}_2 = \mathbf{b}_2$. Par conséquent, la somme $\mathcal{L} + \mathcal{U}$ est directe. □

THÉORÈME 2.2. *La somme des sous-espaces $\mathcal{L}_1, \ldots, \mathcal{L}_m$ de l'espace vectoriel est une somme directe si pour tous vecteurs $\mathbf{a}_1$ de $L_1 \ldots$ $\ldots, \mathbf{a}_m$ de L_m l'égalité*

$$\mathbf{a}_1 + \ldots + \mathbf{a}_m = \mathbf{0} \tag{1}$$

implique les égalités

$$\mathbf{a}_1 = \mathbf{0}, \ldots, \mathbf{a}_m = \mathbf{0}. \tag{2}$$

Démonstration. Supposons que la somme $\mathcal{L}_1 + \ldots$ $\ldots + \mathcal{L}_m$ est directe. Alors de l'égalité (1), qu'on peut écrire sous forme $\mathbf{a}_1 + \ldots + \mathbf{a}_m = \mathbf{0} + \ldots + \mathbf{0}$, s'ensuivent les égalités $\mathbf{a}_1 = \mathbf{0}, \ldots, \mathbf{a}_m = \mathbf{0}$.

Admettons maintenant que pour tous vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ respectivement de $L_1, \ldots, L_m$, l'égalité (1) entraîne les égalités (2). Quels que soient les vecteurs $\mathbf{b}_1, \mathbf{c}_1$ de $L_1, \ldots, \mathbf{b}_m, \mathbf{c}_m$ de L_m l'égalité

$$\mathbf{b}_1 + \ldots + \mathbf{b}_m = \mathbf{c}_1 + \ldots + \mathbf{c}_m \tag{3}$$

implique $(\mathbf{b}_1 - \mathbf{c}_1) + \ldots + (\mathbf{b}_m - \mathbf{c}_m) = 0$, d'où, suivant l'hypothèse, s'ensuivent les égalités

$$\mathbf{b}_1 - \mathbf{c}_1 = 0, \ldots, \mathbf{b}_m - \mathbf{c}_m = 0.$$

Ainsi, de (3) s'ensuivent les égalités

$$\mathbf{b}_1 = \mathbf{c}_1, \ldots, \mathbf{b}_m = \mathbf{c}_m.$$

Par conséquent, la somme $\mathscr{L}_1 + \ldots + \mathscr{L}_m$ est directe. □

Variétés linéaires. Soient $\mathscr{L}$ un sous-espace de l'espace vectoriel $\mathscr{V}$ et L son ensemble de base. Définissons sur l'ensemble V la relation binaire $\sim$ en posant que $a \sim b$ si et seulement si $\mathbf{a} - \mathbf{b} \in L$. Appelons cette relation binaire *congruence en* $\mathscr{L}$.

PROPOSITION 2.3. *Une congruence sur l'ensemble V en $\mathscr{L}$ est une relation d'équivalence sur V.*

Démonstration. La congruence en $\mathscr{L}$ est apparemment réflexive. La relation en $\mathscr{L}$ est symétrique, car de $\mathbf{a} - \mathbf{b} \in L$ s'ensuit $\mathbf{b} - \mathbf{a} \in L$. La congruence en $\mathscr{L}$ est transitive, car pour tous $\mathbf{a}, \mathbf{b}, \mathbf{c} \in V$, de $\mathbf{a} - \mathbf{b} \in L$ et $\mathbf{b} - \mathbf{c} \in L$ s'ensuit $\mathbf{a} - \mathbf{c} = (\mathbf{a} - \mathbf{b}) + (\mathbf{b} - \mathbf{c}) \in L$. Par conséquent, la congruence en $\mathscr{L}$ est une relation d'équivalence sur l'ensemble V. □

La relation d'équivalence $\sim$ sur V définit la partition de l'ensemble V en classes d'équivalence.

DÉFINITION. Soit $\mathscr{L}$ un sous-espace de l'espace vectoriel $\mathscr{V}$. Toute classe d'équivalence de la congruence en $\mathscr{L}$ est appelée *variété linéaire de l'espace* $\mathscr{V}$ *de direction* $\mathscr{L}$.

Exemple. L'ensemble de toutes les solutions d'un système compatible d'équations linéaires à n variables est une variété linéaire de direction $\mathscr{L}$ d'un espace vectoriel arithmétique à n dimensions, où $\mathscr{L}$ est l'espace des solutions du système d'équations homogène correspondant.

De la définition donnée plus haut découlent les propriétés 2.7 et 2.8.

PROPRIÉTÉ 2.7. *Deux vecteurs de l'espace vectoriel $\mathscr{V}$ appartiennent à une même variété linéaire de direction $\mathscr{L}$ si et seulement si leur différence appartient à L.*

PROPRIÉTÉ 2.8. *Toutes deux variétés linéaires de l'espace vectoriel $\mathscr{V}$ de direction $\mathscr{L}$ sont soit coïncidentes, soit disjointes. La réunion de toutes les variétés linéaires de l'espace $\mathscr{V}$ de direction $\mathscr{L}$ est égale à l'ensemble V.*

Notons $\mathbf{a} + L$ $(\mathbf{a} \in V)$ l'ensemble $\{\mathbf{a} + \mathbf{x} \mid \mathbf{x} \in L\}$.

PROPRIÉTÉ 2.9. *Si H est une variété linéaire de l'espace vectoriel $\mathscr{V}$ de direction $\mathscr{L}$ et $\mathbf{a} \in H$, alors $H = \mathbf{a} + L$.*

Démonstration. Vu que tout élément de l'ensemble $\mathbf{a} + L$ est comparable à $\mathbf{a}$ en $\mathscr{L}$, on a $\mathbf{a} + L \subset H$. En outre, tout élément $\mathbf{c}$ de H est comparable à $\mathbf{a}$ en L, et on a $\mathbf{c} - \mathbf{a} \in L$ et $\mathbf{c} \in \mathbf{a} + L$. Donc, $H \subset \mathbf{a} + L$. Par conséquent, $H = \mathbf{a} + L$. □

COROLLAIRE 2.4. *Si* **a** *et* **b** *sont des éléments d'une même variété linéaire de l'espace* $\mathcal{V}$ *de direction* $\mathcal{L}$, *on a alors* $\mathbf{a} + L = \mathbf{b} + L$.

COROLLAIRE 2.5. *Si* $\mathcal{L} \dashv \mathcal{V}$ *et* **c** *un élément quelconque de l'espace* $\mathcal{V}$, $\mathbf{c} + L$ *est alors une variété linéaire de l'espace* $\mathcal{V}$ *de direction* $\mathcal{L}$.

PROPRIÉTÉ 2.10. *Soient* $\mathcal{L}$ *et* $\mathcal{U}$ *des sous-espaces de l'espace vectoriel* $\mathcal{V}$ *et* $\mathbf{a}, \mathbf{b} \in V$. *L'inclusion* $\mathbf{a} + L \subset \mathbf{b} + U$ *a lieu si et seulement si* $\mathbf{a} - \mathbf{b} \in U$ *et* $L \subset U$.

Démonstration. Supposons que $\mathbf{a} + L \subset \mathbf{b} + U$. Alors, $\mathbf{a} \in \mathbf{b} + U$, $\mathbf{a} - \mathbf{b} \in U$ et $\mathbf{a} + U = \mathbf{b} + U$, donc, $\mathbf{a} + L \subset \mathbf{a} + U$ et $L \subset U$.

Admettons maintenant que sont satisfaites les conditions $\mathbf{a} - \mathbf{b} \in U$, $L \subset U$. Alors, $\mathbf{a} + U = \mathbf{b} + U$ et $\mathbf{a} + L \subset \mathbf{a} + U$; donc, $\mathbf{a} + L \subset \mathbf{b} + U$. □

PROPRIÉTÉ 2.11. *Une intersection des variétés linéaires* $\mathbf{a} + L$ *et* $\mathbf{b} + U$ *d'un espace vectoriel n'est pas vide si et seulement si* $\mathbf{a} - \mathbf{b} \in L + U$.

Démonstration. Supposons que l'intersection $\mathbf{a} + L \cap \mathbf{b} + U$ n'est pas vide et **c** est un élément de l'intersection. Alors, $\mathbf{c} = \mathbf{a} + \mathbf{l} = \mathbf{b} + \mathbf{u}$, où $\mathbf{l} \in L$ et $\mathbf{u} \in U$; donc $\mathbf{a} - \mathbf{b} = -\mathbf{l} + \mathbf{u}$ et $\mathbf{a} - \mathbf{b} \in L + U$.

Admettons maintenant que $\mathbf{a} - \mathbf{b} \in L + U$. On a alors $\mathbf{a} - \mathbf{b} = \mathbf{v} + \mathbf{u}$, où $\mathbf{v} \in L$, $\mathbf{u} \in U$ et $\mathbf{a} + (-\mathbf{v}) = \mathbf{b} + \mathbf{u}$. Par conséquent, les variétés $\mathbf{a} + L$ et $\mathbf{b} + U$ ont un élément commun $\mathbf{b} + \mathbf{u}$. □

PROPRIÉTÉ 2.12. *Si l'intersection de la variété linéaire de direction* $\mathcal{L}$ *et de la variété linéaire de direction* $\mathcal{U}$ *n'est pas vide, elle constitue alors une variété linéaire de direction* $\mathcal{L} \cap \mathcal{U}$.

Démonstration. Supposons que l'intersection des variétés $\mathbf{a} + L$ et $\mathbf{b} + U$ n'est pas vide et que **c** est leur élément commun; dans ce cas $\mathbf{a} + L = \mathbf{c} + L$, $\mathbf{b} + U = \mathbf{c} + U$ et $\mathbf{a} + L \cap \mathbf{b} + U = \mathbf{c} + L \cap \mathbf{c} + U$. On vérifie sans peine que $\mathbf{c} + L \cap \mathbf{c} + U = \mathbf{c} + (L \cap U)$. Donc, $\mathbf{a} + L \cap \mathbf{b} + U = \mathbf{c}\,(L \cap U)$, c'est-à-dire que l'intersection des deux variétés envisagées est une variété linéaire de direction $\mathcal{L} \cap \mathcal{U}$. □

PROPRIÉTÉ 2.13. *Si un espace vectoriel* $\mathcal{V}$ *est une somme directe des sous-espaces* $\mathcal{L}$ *et* $\mathcal{U}$, *l'intersection des variétés linéaires de direction* $\mathcal{L}$ *et de direction* $\mathcal{U}$ *ne comporte alors qu'un seul élément.*

Démonstration. Soit $\mathcal{V} = \mathcal{L} \oplus \mathcal{U}$, alors $V = L + U$, $L \cap U = \{\mathbf{0}\}$. Soient $\mathbf{a} + L$ et $\mathbf{b} + U$ des variétés linéaires de directions $\mathcal{L}$ et $\mathcal{U}$ respectivement. Selon la propriété 2.11, leur intersection n'est pas vide, car $\mathbf{a} - \mathbf{b} \in V = L + U$. Soit **c** l'élément commun de l'intersection. Selon la propriété 2.12, il s'ensuit que $\mathbf{a} + L \cap \mathbf{b} + U = \mathbf{c} + (L \cap U) = \mathbf{c} + \{\mathbf{0}\} = \mathbf{c}$. □

Exercices

1. Chacune des conditions suivantes dégage de l'espace vectoriel $\mathcal{V} = \mathcal{F}^n$ des ensembles de vecteurs $(x_1, \ldots, x_n)$. Lesquels de ces ensembles sont fermés dans $\mathcal{V}$ par rapport à l'addition et la multiplication par des scalaires:

(a) $x_1 + x_2 + \ldots + x_n = 0$; (e) $x_1 = 1$;

(b) $x_1 + x_2 + \ldots + x_n = 1$; (f) $x_1 = x_n = 0$;

(c) $x_1 - x_2 - \ldots - x_n = 0$; (g) $x_1 \cdot x_n = 0$;

(d) $x_n = 0$; (h) $x_1 = x_2 = \ldots = x_n$?

2. Soit $\mathcal{V} = \mathcal{F}^{n \times n}$ l'espace vectoriel de toutes les matrices $n \times n$ sur un corps. Montrer que l'ensemble de toutes les matrices symétriques (symétriques gauches) de l'espace $\mathcal{V}$ est un sous-espace de l'espace $\mathcal{V}$ par rapport à l'addition et la multiplication par des scalaires.

3. Soient $\mathcal{V} = \mathcal{F}^{n \times n}$ sur le corps numérique $\mathcal{F}$, $\mathcal{L}$ un sous-espace de toutes les matrices $n \times n$ symétriques et $\mathcal{U}$ un sous-espace de toutes les matrices symétriques gauches. Démontrer que $\mathcal{V} = \mathcal{L} \oplus \mathcal{U}$.

4. Soit $\mathcal{V}$ un espace vectoriel (sur $\mathcal{R}$) de toutes les fonctions f trois fois dérivables: $\mathbf{R} \to \mathbf{R}$, satisfaisant à la condition $f''' + f' = 0$. Montrer que l'ensemble de toutes les fonctions de l'espace, satisfaisant à la condition $f'' + f = 0$, constitue un sous-espace de l'espace $\mathcal{V}$.

5. Soit $\mathcal{V} = \mathcal{R}^{2\times 2}$ un espace vectoriel des matrices 2×2 sur le corps $\mathcal{R}$ des nombres réels. Montrer que l'ensemble de toutes les matrices sur $\mathcal{R}$ de l'aspect $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ constitue un sous-espace de l'espace $\mathcal{V}$.

6. Soient $\mathbf{a}_1, \ldots, \mathbf{a}_k, \mathbf{b}_1, \ldots, \mathbf{b}_s$ des vecteurs de l'espace vectoriel $\mathcal{V}$. Démontrer que

$$L(\mathbf{a}_1, \ldots, \mathbf{a}_k) + L(\mathbf{b}_1, \ldots, \mathbf{b}_s) = L(\mathbf{a}_1, \ldots, \mathbf{a}_k, \mathbf{b}_1, \ldots, \mathbf{b}_s).$$

7. Démontrer que l'intersection de tout ensemble de sous-espaces de l'espace vectoriel $\mathcal{V}$ est un sous-espace de l'espace $\mathcal{V}$.

8. Soient $\mathcal{L}$ et $\mathcal{U}$ des sous-espaces de l'espace vectoriel $\mathcal{V}$. Démontrer que $\mathcal{L} + \mathcal{U}$ est une intersection de tous les sous-espaces de l'espace $\mathcal{V}$ contenant les sous-espaces $\mathcal{L}$ et $\mathcal{U}$.

9. Soient $\mathbf{a}, \mathbf{b}, \mathbf{c}$ des vecteurs satisfaisant à la condition $\mathbf{a} + \lambda\mathbf{b} + \xi\mathbf{c} = \mathbf{0}$, où λ, ξ sont des scalaires non nuls. Montrer que $L(\mathbf{a}, \mathbf{b}) = L(\mathbf{b}, \mathbf{c}) = L(\mathbf{c}, \mathbf{a})$.

10. Supposons que les vecteurs $\mathbf{a}, \mathbf{b}$ sont linéairement indépendants. Montrer que $\mathcal{L}(\mathbf{a}, \mathbf{b}) = \mathcal{L}(\mathbf{a}) \oplus \mathcal{L}(\mathbf{b})$.

11. Soit un système des vecteurs $\mathbf{a}, \mathbf{b}, \mathbf{c}$ linéairement indépendant. Démontrer que $\mathcal{L}(\mathbf{a}, \mathbf{b}, \mathbf{c}) = \mathcal{L}(\mathbf{a}) \oplus \mathcal{L}(\mathbf{b}) \oplus \mathcal{L}(\mathbf{c})$.

12. Montrer que si le vecteur $\mathbf{b}$ est une combinaison linéaire des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$, alors $L(\mathbf{a}_1, \ldots, \mathbf{a}_m) = L(\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b})$.

13. Supposons que l'espace vectoriel $\mathcal{V}$ est engendré par le sous-espace $\mathcal{U}$ et le vecteur $\mathbf{a}$. Montrer que si $\mathbf{b} \in V \setminus U$, alors $\mathcal{V} = \mathcal{U} \oplus \mathcal{L}(\mathbf{b})$.

14. Soit $\mathcal{V}$ la somme des sous-espaces $\mathcal{L}$ et $\mathcal{U}$. Montrer que $\mathcal{V} = \mathcal{L} \oplus \mathcal{U}$ si peut être représenté de façon unique au moins un vecteur $\mathbf{c} \in V$ sous forme de $\mathbf{c} = \mathbf{a} + \mathbf{b}$, où $\mathbf{a} \in L$, $\mathbf{b} \in U$.

15. Soit $\mathcal{V}$ une somme directe des sous-espaces $\mathcal{L}$ et $\mathcal{U}$. Montrer que si $\mathbf{a}_1, \ldots, \mathbf{a}_m$ est un système linéairement indépendant de vecteurs du sous-espace $\mathcal{L}$, et $\mathbf{b}_1, \ldots, \mathbf{b}_s$ un système linéairement indépendant de vecteurs de $\mathcal{U}$, alors $\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}_1, \ldots, \mathbf{b}_s$ est un système linéairement indépendant de vecteurs de l'espace $\mathcal{V}$.

16. Soit $\mathcal{V}$ un espace vectoriel, somme des sous-espaces $\mathcal{L}_1$, $\mathcal{L}_2$, $\mathcal{L}_3$. Démontrer que $\mathcal{V} = \mathcal{L}_1 \oplus \mathcal{L}_2 \oplus \mathcal{L}_3$ si et seulement si $L_1 \cap L_2 = \mathbf{0}$ et $(L_1 + L_2) \cap L_3 = \mathbf{0}$.

17. Soient $\mathcal{V}^0 = \mathcal{F}^n$, où $\mathcal{F}$ est un corps des scalaires composé de deux éléments, et $\mathbf{b}_1, \ldots, \mathbf{b}_m$ un système linéairement indépendant de vecteurs de l'espace $\mathcal{V}^0$. Combien de vecteurs comporte l'enveloppe linéaire $L(\mathbf{b}_1, \ldots, \mathbf{b}_m)$ de ces vecteurs?

§ 3. Base et dimension de l'espace vectoriel

Base de l'espace vectoriel. Soit $\mathcal{V}$ un espace vectoriel avec l'ensemble de base V. S'il existe dans V un ensemble fini $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ de vecteurs tel que $V = L(\mathbf{a}_1, \ldots, \mathbf{a}_m)$, on dit alors que l'espace $\mathcal{V}$ est engendré par l'ensemble fini $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ qu'on appellera *ensemble* (ou système) *engendrant les espaces* $\mathcal{V}$.

DÉFINITION. Un espace vectoriel est dit *de dimension finie* s'il est engendré par un ensemble fini de vecteurs.

DÉFINITION. On appelle *base d'un espace de vecteurs de dimension finie* un système de vecteurs non vide, fini et linéairement indépendant engendrant cet espace.

Exemple. Soit $\mathcal{V} = \mathcal{F}^n$ un espace vectoriel arithmétique sur le corps $\mathcal{F}$. Le système des vecteurs unités

$$\mathbf{e}_1 = (1, 0, \ldots, 0), \ldots, \mathbf{e}_n = (0, 0, \ldots, 0, 1)$$

est linéairement indépendant et engendre l'espace $\mathcal{V}$, c'est-à-dire $V = L(\mathbf{e}_1, \ldots, \mathbf{e}_n)$. Par conséquent, le système des vecteurs $\mathbf{e}_1, \ldots, \mathbf{e}_n$ constitue la base de l'espace $\mathcal{F}^n$.

THÉORÈME 3.1. *Tout espace vectoriel* $\neq \{0\}$ *et de dimension finie possède une base. En outre, si le système des vecteurs*

$$(1) \quad \mathbf{a}_1, \ldots, \mathbf{a}_m$$

engendre l'espace vectoriel $\mathcal{V}$, *alors la base du système des vecteurs* (1) *est la base de l'espace* $\mathcal{V}$.

Démonstration. Supposons que l'espace $\mathcal{V}$ est engendré par le système des vecteurs (1), c'est-à-dire $V = L(\mathbf{a}_1, \ldots, \mathbf{a}_m)$; on peut estimer que les vecteurs du système (1) ne sont pas nuls. Selon le théorème 5.1, le système (1) a une base. Soit

$$(2) \quad \mathbf{b}_1, \ldots, \mathbf{b}_n$$

la base du système (1). Le système (2) engendre alors aussi l'espace $\mathcal{V}$, c'est-à-dire $V = L(\mathbf{b}_1, \ldots, \mathbf{b}_n)$. De plus, le système (2) est linéairement indépendant. Par conséquent, le système (2) est la base du système (1) et, partant, la base de l'espace $\mathcal{V}$. □

THÉORÈME 3.2. *Soit* $\mathcal{V}$ *un espace vectoriel* $\neq \{0\}$ *et de dimension finie. Alors, le nombre d'éléments d'une base de l'espace* $\mathcal{V}$ *vaut le nombre d'éléments de toute autre base de cet espace.*

Démonstration. Selon le théorème 3.1, l'espace $\mathcal{V}$ possède une base. Soient

$$(1) \quad \mathbf{b}_1, \ldots, \mathbf{b}_n$$

une base de l'espace $\mathcal{V}$ et

(2) $\mathbf{c}_1, \ldots, \mathbf{c}_s$

toute autre base de cet espace. Alors, $V = L(\mathbf{b}_1, \ldots, \mathbf{b}_n) = L(\mathbf{c}_1, \ldots, \mathbf{c}_s)$. Les systèmes de vecteurs (1) et (2) sont donc équivalents. Donc, selon le théorème 5.1.2, $n = s$. □

COROLLAIRE 3.3. *Si la base de l'espace vectoriel $\mathcal{V}$ est composée de n éléments, alors, pour $k > n$ tout système de k vecteurs de l'espace $\mathcal{V}$ est linéairement dépendant.*

Démonstration. Si $\mathbf{b}_1, \ldots, \mathbf{b}_n$ est une base de l'espace $\mathcal{V}$ et $\mathbf{a}_1, \ldots, \mathbf{a}_k$ des vecteurs quelconques de V, alors $\mathbf{a}_1, \ldots, \mathbf{a}_k \in L(\mathbf{b}_1, \ldots, \mathbf{b}_n)$. Il s'ensuit, selon le théorème 5.1, pour $k > n$, que le système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_k$ est linéairement dépendant. □

COROLLAIRE 3.4. *Si la base de l'espace vectoriel $\mathcal{V}$ comporte n vecteurs, alors tout système de n vecteurs engendrant l'espace $\mathcal{V}$ est une base de cet espace.*

THÉORÈME 3.5. *Tout sous-espace $\mathcal{U}$ d'un espace vectoriel de dimension finie $\mathcal{V}$ est de dimension finie. Si $\mathcal{V}$ possède une base composée de n éléments et $\mathcal{U}$ est un sous-espace $\neq \{0\}$, alors $\mathcal{U}$ possède une base dont le nombre d'éléments est inférieur ou égal à n.*

Démonstration. Soient $\mathcal{V}$ un espace vectoriel de dimension finie et $\mathcal{U}$ son sous-espace. Si $\mathcal{U}$ est un sous-espace $= \{0\}$, il est alors de dimension finie. Supposons que le sous-espace $\mathcal{U}$ est $\neq \{0\}$. Alors $\mathcal{V}$ est un espace $\neq \{0\}$ et, selon le théorème 3.1, possède une base. Posons que la base de l'espace $\mathcal{V}$ comporte n éléments. Alors, tout système de vecteurs linéairement indépendant de l'espace $\mathcal{V}$ contient n éléments au plus.

Soit $\mathbf{u}_1$ un élément non nul de l'espace $\mathcal{U}$. Si $U \neq L(\mathbf{u}_1)$, il existe un vecteur $\mathbf{u}_2 \in U - L(\mathbf{u}_1)$, le système des vecteurs $\mathbf{u}_1, \mathbf{u}_2$ étant linéairement indépendant. Si $U \neq L(\mathbf{u}_1, \mathbf{u}_2)$, il existe un vecteur $\mathbf{u}_3 \in U \setminus L(\mathbf{u}_1, \mathbf{u}_2)$, le système des vecteurs $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ étant linéairement indépendant. En continuant de la sorte, on aboutit à la suite

(1) $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \ldots$

d'éléments linéairement indépendants de l'espace $\mathcal{U}$. Cette suite comporte n éléments au plus. Il existe donc un nombre naturel $m \leqslant n$ $(m > 0)$ tel que $U = L(\mathbf{u}_1, \ldots, \mathbf{u}_m)$. Le sous-espace $\mathcal{U}$ est ainsi de dimension finie et le système des vecteurs $\mathbf{u}_1, \ldots, \mathbf{u}_m$ est sa base. □

Complétion jusqu'à la base d'un système de vecteurs indépendant. Est-il possible d'inclure dans toute base un système quelconque de vecteurs linéairement indépendant?

THÉORÈME 3.6. *Un système de vecteurs linéairement indépendant de l'espace vectoriel $\mathcal{V}$ de dimension finie et $\neq \{0\}$ ne constituant pas*

une base de l'espace peut être complété jusqu'à la base de l'espace $\mathscr{V}$.

D é m o n s t r a t i o n. Soit

(1) $\mathbf{a}_1, \ldots, \mathbf{a}_m$

un système linéairement indépendant ne constituant pas une base de l'espace $\mathscr{V}$. Soit $\mathbf{b}_1, \ldots, \mathbf{b}_n$ la base de l'espace $\mathscr{V}$. Considérons le système

(S) $\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}_1, \ldots, \mathbf{b}_n$.

Selon le corollaire 3.3, ce système est linéairement dépendant. Donc, un au moins des vecteurs $\mathbf{b}_1, \ldots, \mathbf{b}_n$ est une combinaison linéaire des vecteurs qui le précèdent dans le système (S). Eliminons un de ces vecteurs du système (S); on obtient le système

(S_1) $\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}_1^{(1)}, \ldots, \mathbf{b}_{n-1}^{(1)}$,

équivalent au système (S) et, par suite, générateur de l'espace $\mathscr{V}$. Si (S_1) comporte plus de n éléments, alors, (selon le corollaire 3.3) il est linéairement dépendant et, partant, un des éléments $\mathbf{b}_1^{(1)}, \ldots$ $\ldots, \mathbf{b}_{n-1}^{(1)}$ est une combinaison linéaire des éléments précédents. Supprimons cet élément de (S_1). On obtient alors le système (S_2) équivalent au système (S) et, par suite, générateur de l'espace $\mathscr{V}$. En poursuivant l'opération après m éliminations on aboutit au système den vecteurs

(S_m) $\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}_1^{(m)}, \ldots, \mathbf{b}_{n-m}^{(m)}$,

équivalent au système (S) et donc engendrant l'espace $\mathscr{V}$. Selon le corollaire 3.4 le système (S_m) est la base de l'espace $\mathscr{V}$. Comme le système (S_m) contient le système de départ (1), le système (S_m) est la base cherchée de l'espace $\mathscr{V}$. □

THÉORÈME 3.7. *Si $\mathscr{U}$ est un sous-espace de l'espace vectoriel $\mathscr{V}$ de dimension finie, il existe alors un sous-espace $\mathscr{W}$ de l'espace $\mathscr{V}$, tel que*

(1) $\mathscr{V} = \mathscr{U} \oplus \mathscr{W}$.

D é m o n s t r a t i o n. L'égalité (1) est vraie si $\mathscr{U}$ est un sous-espace trivial, c'est-à-dire un sous-espace $= \{0\}$ ou un sous-espace coïncidant avec $\mathscr{V}$. Supposons que $\mathscr{U}$ est un sous-espace non trivial et

(2) $\mathbf{a}_1, \ldots, \mathbf{a}_m$

est sa base. Selon le théorème 3.6 le système (2) peut être complété jusqu'à la base de l'espace $\mathscr{V}$, c'est-à-dire qu'il existe des vecteurs $\mathbf{a}_{m+1}, \ldots, \mathbf{a}_n$ pour lesquels le système

(3) $\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{a}_{m+1}, \ldots, \mathbf{a}_n$

devient la base de l'espace $\mathscr{V}$. Alors,

(4) $V = U + W$,

où $W = L(\mathbf{a}_{m+1}, \ldots, \mathbf{a}_n)$. Démontrons que

(5) $U \cap W = \{\mathbf{0}\}$.

En effet, si $\mathbf{c} \in U \cap W$, alors

$$\mathbf{c} = \alpha_1\mathbf{a}_1 + \ldots + \alpha_m\mathbf{a}_m \in U, \quad \mathbf{c} = \alpha_{m+1}\mathbf{a}_{m+1} + \ldots + \alpha_n\mathbf{a}_n \in W$$

et, par suite,

$$\alpha_1\mathbf{a}_1 + \ldots + \alpha_m\mathbf{a}_m + (-\alpha_{m+1})\,\mathbf{a}_{m+1} + \ldots + (-\alpha_n)\,\mathbf{a}_n = \mathbf{0}.$$

En vertu de l'indépendance linéaire du système (3), tous les coefficients s'annulent et, en particulier, $\alpha_1 = 0, \ldots, \alpha_m = 0$. Par conséquent, $\mathbf{c} = \mathbf{0}$, c'est-à-dire (5) se vérifie.

Sur la base de (4) et (5) on conclut que pour $\mathscr{W} = \mathscr{L}(\mathbf{a}_{m+1}, \ldots, \mathbf{a}_n)$ on a l'égalité (1). □

COROLLAIRE 3.8. Si le système (3) est la base de l'espace $\mathscr{V}$, alors

$$\mathscr{V} = \mathscr{L}(\mathbf{a}_1, \ldots, \mathbf{a}_m) \oplus \mathscr{L}(\mathbf{a}_{m+1}, \ldots, \mathbf{a}_n).$$

Dimension de l'espace vectoriel. Un des plus importants invariants de l'espace vectoriel est sa dimension.

DÉFINITION. On appelle *dimension de l'espace vectoriel de dimension finie* $\neq \{\mathbf{0}\}$ le nombre de vecteurs d'une base quelconque de l'espace. La dimension d'un espace vectoriel $= \{\mathbf{0}\}$ est par convention égale à zéro. La dimension de l'espace vectoriel est désignée par $\dim \mathscr{V}$.

E x e m p l e. Soit $\mathscr{F}^n$ un espace vectoriel arithmétique sur le corps $\mathscr{F}$. Les vecteurs $\mathbf{e}_1 = (1, 0, \ldots, 0)$, $\mathbf{e}_2 = (0, 1, 0, \ldots, 0), \ldots, \mathbf{e}_n = (0, 0, \ldots, 0, 1)$ constituent la base de l'espace. Par conséquent, $\dim \mathscr{F}^n = n$.

Considérons quelques propriétés de la dimension.

PROPRIÉTÉ 3.1. Si $\mathscr{V}$ est un espace vectoriel de dimension finie et $\dim \mathscr{V} = n$, alors, pour $k > n$, tout système de k vecteurs de l'espace $\mathscr{V}$ est linéairement dépendant.

D é m o n s t r a t i o n. Si $n = 0$, alors $\mathscr{V} = \{\mathbf{0}\}$ et la propriété 3.1 est vérifiée. Mais si $\dim \mathscr{V} = n > 0$, la base de l'espace $\mathscr{V}$ est alors constituée de n vecteurs. Selon la propriété 3.3, on en déduit que pour $k > n$ tout système de k vecteurs de l'espace $\mathscr{V}$ est linéairement dépendant. □

COROLLAIRE 3.9. *Si* $\dim \mathscr{V} = n$ *et le système des vecteurs* $\mathbf{b}_1, \ldots, \mathbf{b}_m$ *de l'espace* $\mathscr{V}$ *est linéairement indépendant, alors* $m \leqslant n$.

PROPRIÉTÉ 3.2. *Si* $\mathscr{U}$ *est un sous-espace d'un espace vectoriel de dimension finie* $\mathscr{V}$, *alors*

(1) $\dim \mathscr{U} \leqslant \dim \mathscr{V}$.

D é m o n s t r a t i o n. L'inégalité (1) est apparemment vraie si $\mathscr{U} = \{\mathbf{0}\}$. Mais si le sous-espace $\neq \{\mathbf{0}\}$, alors (selon le théorème 3.5) il est de dimension finie et (selon le théorème 3.1) a une

base. Soit $\mathbf{b}_1, \ldots, \mathbf{b}_m$ la base du sous-espace $\mathcal{U}$. Alors, $\dim \mathcal{U} = m$. Dans l'espace $\mathcal{V}$ le système des vecteurs $\mathbf{b}_1, \ldots, \mathbf{b}_m$ est linéairement indépendant. Donc, selon le corollaire 3.9 $m \leqslant n$. □

PROPRIÉTÉ 3.3. *Si $\mathcal{U}$ est un sous-espace de l'espace vectoriel de dimension finie et* $\dim \mathcal{U} = \dim \mathcal{V}$, *on a alors* $\mathcal{U} = \mathcal{V}$.

D é m o n s t r a t i o n. Si le sous-espace $\mathcal{U} = \{\mathbf{0}\}$, alors $\dim \mathcal{U} = 0$. Par suite, en vertu de l'hypothèse $\dim \mathcal{V} = 0$. Donc $\mathcal{V}$ est également un espace vectoriel égal à $\{\mathbf{0}\}$. Par conséquent, $\mathcal{U} = \mathcal{V}$.

Supposons que $\mathcal{U} \neq \{\mathbf{0}\}$. Il est alors de même que $\mathcal{V}$, de dimension finie et, selon le théorème 3.1, possède une base. Soit $\mathbf{b}_1, \ldots, \mathbf{b}_n$ sa base. On a alors $\dim \mathcal{U} = n$ et, par hypothèse, $\dim \mathcal{V} = n$. Le système $\mathbf{b}_1, \ldots, \mathbf{b}_n$ est donc également une base de l'espace $\mathcal{V}$. Par conséquent, $\mathcal{U} = \mathcal{V}$. □

PROPRIÉTÉ 3.4. *Si l'espace vectoriel de dimension finie $\mathcal{V}$ est une somme directe des sous-espaces $\mathcal{U}$ et $\mathcal{L}$, alors*

(1) $\dim \mathcal{V} = \dim \mathcal{U} + \dim \mathcal{L}$.

D é m o n s t r a t i o n. Par hypothèse $\mathcal{V} = \mathcal{U} \oplus \mathcal{L}$ et, par suite,

(2) $U \cap L = \{\mathbf{0}\}$,

(3) $V = U + L$.

Si $\mathcal{U}$ ou $\mathcal{L}$ sont égaux à $\{\mathbf{0}\}$, l'égalité (1) est apparemment vraie.

Supposons que $\mathcal{U}$ et $\mathcal{L}$ sont $\neq \{\mathbf{0}\}$. Soient

(4) $\mathbf{b}_1, \ldots, \mathbf{b}_m$,

(5) $\mathbf{b}_{m+1}, \ldots, \mathbf{b}_{m+s}$

des bases des espaces $\mathcal{U}$ et $\mathcal{L}$ respectivement. Démontrons que le système

(6) $\mathbf{b}_1, \ldots, \mathbf{b}_m, \mathbf{b}_{m+1}, \ldots, \mathbf{b}_{m+s}$

est une base de l'espace $\mathcal{V}$. En vertu de (2), on a

(7) $L(\mathbf{b}_1, \ldots, \mathbf{b}_m) \cap L(\mathbf{b}_{m+1}, \ldots, \mathbf{b}_{m+s}) = \{\mathbf{0}\}$.

Le système (6) est linéairement indépendant. En effet, pour tous scalaires $\lambda_1, \ldots, \lambda_{m+s}$ de l'égalité

$$\lambda_1\mathbf{b}_1 + \ldots + \lambda_m\mathbf{b}_m + \lambda_{m+1}\mathbf{b}_{m+1} + \ldots + \lambda_{m+s}\mathbf{b}_{m+s} = \mathbf{0},$$

en vertu de (7), s'ensuivent les égalités

(8) $\lambda_1\mathbf{b}_1 + \ldots + \lambda_m\mathbf{b}_m = \mathbf{0}, \quad \lambda_{m+1}\mathbf{b}_{m+1} + \ldots + \lambda_{m+s}\mathbf{b}_{m+s} = \mathbf{0}$,

et comme les systèmes (4) et (5) sont linéairement indépendants, il s'ensuit de (8) que $\lambda_1 = 0, \ldots, \lambda_m = 0, \ldots, \lambda_{m+s} = 0$. Ensui-

te, en vertu de (3),

$$V = U + L = L(\mathbf{b}_1, \ldots, \mathbf{b}_m) + L(\mathbf{b}_{m+1}, \ldots, \mathbf{b}_{m+s}) = \\ = L(\mathbf{b}_1, \ldots, \mathbf{b}_m, \mathbf{b}_{m+1}, \ldots, \mathbf{b}_{m+s}),$$

autrement dit, le système (6) engendre l'espace $\mathscr{V}$. Bref, on a démontré que le système (6) est une base de l'espace $\mathscr{V}$. Par conséquent, $\dim \mathscr{V} = m + s = \dim \mathscr{U} + \dim \mathscr{L}$. □

Théorème 3.10. *Si l'espace vectoriel $\mathscr{V}$ est une somme des sous-espaces de dimension finie $\mathscr{U}$ et $\mathscr{L}$, alors*

(1) $\dim (\mathscr{U} + \mathscr{L}) + \dim (\mathscr{U} \cap \mathscr{L}) = \dim \mathscr{U} + \dim \mathscr{L}$.

Démonstration. Supposons que

(2) $\mathscr{V} = \mathscr{U} + \mathscr{L}$.

Si $U \cap L = \{\mathbf{0}\}$, la somme (2) est alors directe; donc, selon la propriété 3.4, le théorème est vrai. □

Supposons que $U \cap L \neq \varnothing$. Alors l'espace $\mathscr{U} \cap \mathscr{L}$, de même que $\mathscr{U}$, est de dimension finie. Soit

(2) $\mathbf{b}_1, \ldots, \mathbf{b}_s$

la base de l'espace $\mathscr{U} \cap \mathscr{L}$. Complétons-la jusqu'à la base des espaces $\mathscr{U}$ et $\mathscr{L}$. Soient

(3) $\mathbf{b}_1, \ldots, \mathbf{b}_s, \mathbf{b}_{s+1}, \ldots, \mathbf{b}_m$

la base de l'espace $\mathscr{U}$ et

(4) $\mathbf{b}_1, \ldots, \mathbf{b}_s, \mathbf{b}_{m+1}, \ldots, \mathbf{b}_{m+k}$

la base de l'espace $\mathscr{L}$. Alors,

(5) $\dim (\mathscr{U} \cap \mathscr{L}) = s, \ \dim \mathscr{U} = m, \ \dim \mathscr{L} = s + k$

et, par suite,

(6) $U = L(\mathbf{b}_1, \ldots, \mathbf{b}_m), \ \ L = L(\mathbf{b}_1, \ldots, \mathbf{b}_s, \mathbf{b}_{m+1}, \ldots, \mathbf{b}_{m+k})$

De (4) et (6), on dérive que

$$V = U + L = L(\mathbf{b}_1, \ldots, \mathbf{b}_m, \mathbf{b}_{m+1}, \ldots, \mathbf{b}_{m+k}),$$

c'est-à-dire que le système

(7) $\mathbf{b}_1, \ldots, \mathbf{b}_m, \mathbf{b}_{m+1}, \ldots, \mathbf{b}_{m+k}$

engendre l'espace $\mathscr{V}$.

Montrons que le système (7) est linéairement indépendant. Supposons que l'on a

(8) $\lambda_1\mathbf{b}_1 + \ldots + \lambda_s\mathbf{b}_s + \ldots + \lambda_m\mathbf{b}_m + \lambda_{m+1}\mathbf{b}_{m+1} + \ldots \\ \ldots + \lambda_{m+k}\mathbf{b}_{m+k} = \mathbf{0}$.

16—01762

De (6) et (8), on dérive que

$$\lambda_{m+1}\mathbf{b}_{m+1} + \ldots + \lambda_{m+k}\mathbf{b}_{m+k} \in U \cap L$$

et, partant,

$$\lambda_{m+1}\mathbf{b}_{m+1} + \ldots + \lambda_{m+k}\mathbf{b}_{m+k} \in L(\mathbf{b}_1, \ldots, \mathbf{b}_s).$$

En vertu de l'indépendance linéaire du système (5), il s'ensuit que

$$(9) \quad \lambda_{m+1} = 0, \ldots, \lambda_{m+k} = 0.$$

A partir de (8) et de (9) on déduit l'égalité

$$\lambda_1\mathbf{b}_1 + \ldots + \lambda_m\mathbf{b}_m = \mathbf{0}.$$

Vu l'indépendance linéaire du système (3) découle l'égalité

$$\lambda_1 = 0, \ldots, \lambda_m = 0.$$

Bref, on a établi que le système (7) est linéairement indépendant. Ainsi, le système (7) est la base de l'espace $\mathscr{V}$ et

$$(10) \quad \dim(\mathscr{U} + \mathscr{L}) = m + k.$$

En vertu de (5) et (10), on a

$$\dim(\mathscr{U} + \mathscr{L}) + \dim(\mathscr{U} \cap \mathscr{L}) = m + k + s = \dim \mathscr{U} + \dim \mathscr{L}. \quad \square$$

Exercices

1. Montrer que le système des vecteurs (α, β), (γ, δ) d'un espace vectoriel arithmétique à deux dimensions $\mathscr{V}$ est une base de l'espace $\mathscr{V}$ si et seulement si $\alpha\delta - \beta\gamma \neq 0$.

2. Montrer que le système des vecteurs $(1, 1, 1)$, $(0, 1, 1)$ $(1, 0, 1)$ est une base de l'espace $\mathscr{V} = \mathscr{F}^3$. Chercher les lignes de coordonnées des vecteurs unités $\mathbf{e}_1 = (1, 0, 0)$, $\mathbf{e}_2 = (0, 1, 0)$, $\mathbf{e}_3 = (0, 0, 1)$ par rapport à cette base.

3. Montrer que pour des scalaires α, β, γ quelconques le système des vecteurs $(1, \alpha, \beta)$, $(0, 1, \gamma)$, $(0, 0, 1)$ est une base de l'espace $\mathscr{V} = \mathscr{F}^3$.

4. Soit $\mathscr{F}$ un corps numérique. A quelles conditions doivent satisfaire les scalaires $\alpha, \beta, \gamma \in F$ pour que le système des vecteurs $(1, \alpha, \alpha^2)$, $(1, \beta, \beta^2)$, $(1, \gamma, \gamma^2)$ soit une base de l'espace $\mathscr{F}^3$?

5. A quelles conditions doit satisfaire le scalaire λ pour que le système des vecteurs $(\lambda, 1, 0)$, $(1, \lambda, 1)$, $(0, 1, \lambda)$ soit une base de l'espace $\mathscr{C}^3$; de l'espace $\mathfrak{R}^3$?

6. Soit $\mathscr{V}$ un espace vectoriel constituant une somme directe des sous-espaces de dimension finie $\mathscr{L}_1$ et $\mathscr{L}_2$. Montrer qu'après avoir complété la base du sous-espace $\mathscr{L}_2$ par la base du sous-espace $\mathscr{L}_1$ on obtient la base de l'espace $\mathscr{V}$.

7. Soit $\mathscr{F}$ un corps constitué de deux éléments. Combien de bases différentes possède l'espace $\mathscr{F}^3$?

8. Soit $\mathscr{V}$ un espace vectoriel à n dimensions. Démontrer que le système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_n$ est une base de l'espace $\mathscr{V}$ si et seulement si $\mathscr{V} = \mathscr{L}(\mathbf{a}_1, \ldots, \mathbf{a}_n)$.

9. Soit $\mathscr{V} = \mathscr{F}^{m \times n}$ un espace vectoriel des matrices $m \times n$ sur le corps $\mathscr{F}$. Quelles sont sa base et sa dimension?

10. Soit $\mathcal{V}$ un espace vectoriel de dimension finie $\neq \{0\}$. Démontrer que la dimension du sous-espace $\mathcal{L}(\mathbf{a}_1, \ldots, \mathbf{a}_m)$ étalé sur les vecteurs donnés $\mathbf{a}_1, \ldots, \mathbf{a}_m$ de l'espace $\mathcal{V}$ est du rang de la matrice composée avec les lignes de coordonnées des vecteurs envisagés dans une base quelconque.

11. Démontrer que le système $\mathbf{a}_1, \ldots, \mathbf{a}_n$ des vecteurs non nuls de l'espace vectoriel à n dimensions $\mathcal{V}$ n'est une base de l'espace $\mathcal{V}$ que si $\mathbf{a}_k \notin L(\mathbf{a}_1, \ldots, \mathbf{a}_{k-1})$ pour $k = 2, 3, \ldots, n$.

12. Soient $\mathcal{F}$ un corps fini composé de p éléments et $\mathcal{V} = \mathcal{F}^n$. Combien de bases distinctes possède l'espace vectoriel $\mathcal{V}$?

13. Soient $\mathbf{a}_1, \ldots, \mathbf{a}_n$ une base de l'espace vectoriel $\mathcal{V}$ et k un entier positif inférieur à n. Démontrer que $\mathcal{V} = \mathcal{L}(\mathbf{a}_1, \ldots, \mathbf{a}_k) \oplus \mathcal{L}(\mathbf{a}_{k+1}, \ldots, \mathbf{a}_n)$.

14. Soit $\mathbf{e}_1, \ldots, \mathbf{e}_n$ une base standard de l'espace vectoriel $\mathcal{V} = \mathcal{F}^n$. Montrer que le système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_n$ de l'espace $\mathcal{V}$ est une base de l'espace $\mathcal{V}$ si et seulement si $\mathbf{e}_1, \ldots, \mathbf{e}_n \in L(\mathbf{a}_1, \ldots, \mathbf{a}_n)$.

15. Démontrer que si la somme des dimensions de deux sous-espaces d'un espace à n dimensions est supérieure à n, ces sous-espaces possèdent alors un vecteur non nul commun.

16. Démontrer que l'espace vectoriel $\mathcal{V}$ ne possède que deux sous-espaces si et seulement si l'espace $\mathcal{V}$ est à une dimension.

17. Démontrer qu'un espace vectoriel à deux dimensions sur un corps numérique possède un ensemble infini de sous-espaces à une dimension distincts.

18. Soient $\mathcal{V} = \mathcal{U} \oplus \mathcal{L}$, où $\mathcal{V}$ est un espace à trois dimensions, et $\mathcal{U}$, $\mathcal{L}$ des sous-espaces $\{\neq 0\}$ non identiques à $\mathcal{V}$. Montrer que l'un des sous-espaces $\mathcal{U}$, $\mathcal{L}$ est à une dimension, et l'autre à deux dimensions.

19. Soient $\mathcal{L}$ et $\mathcal{U}$ des sous-espaces à une dimension différents d'un espace vectoriel bidimensionnel $\mathcal{V}$. Démontrer que $\mathcal{V} = \mathcal{L} \oplus \mathcal{U}$.

20. Soient $\mathcal{L}$ et $\mathcal{U}$ des sous-espaces à deux dimensions différents d'un espace vectoriel tridimensionnel $\mathcal{V}$. Démontrer que $\mathcal{V} = \mathcal{L} + \mathcal{U}$ et $\mathcal{L} \cap \mathcal{U}$ est un sous-espace unidimensionnel.

21. Soient $\mathcal{L}$ et $\mathcal{U}$ des sous-espaces d'un espace vectoriel à n dimensions $\mathcal{V}$ dont les dimensions sont k et s respectivement. Démontrer que:

(a) si $L \cap V = \{0\}$ et $k + s = n$, alors $\mathcal{V} = \mathcal{L} \oplus \mathcal{U}$;

(b) si $\mathcal{V} = \mathcal{L} + \mathcal{U}$ et $k + s = n$, alors $\mathcal{V} = \mathcal{L} \oplus \mathcal{U}$.

22. Démontrer que l'espace vectoriel à n dimensions peut être représenté, pour $n > 1$, sous forme d'une somme directe de n sous-espaces unidimensionnels.

23. Soit $\mathbf{b}_1, \ldots, \mathbf{b}_n$ la base de l'espace vectoriel $\mathcal{V}$. Montrer que $\mathcal{V} = \mathcal{L}(\mathbf{b}_1) \oplus \ldots \oplus \mathcal{L}(\mathbf{b}_n)$.

24. Soit $\mathcal{V} = \mathcal{L}_1 + \mathcal{L}_2 + \mathcal{L}_3$, où $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$ sont des sous-espaces de l'espace à n dimensions $\mathcal{V}$ dont les dimensions sont r, s, t respectivement. Démontrer que $\mathcal{V} = \mathcal{L}_1 \oplus \mathcal{L}_2 \oplus \mathcal{L}_3$ si et seulement si $r + s + t = n$.

§ 4. Isomorphismes des espaces vectoriels

Ligne de coordonnées d'un vecteur par rapport à une base donnée. Soit $\mathcal{V}$ un espace vectoriel sur le corps $\mathcal{F}$.

THÉORÈME 4.1. *Soit*

(1) $\mathbf{b}_1, \ldots, \mathbf{b}_n$

la base de l'espace vectoriel $\mathcal{V}$. Pour chaque vecteur $\mathbf{a}$ *de V il existe dans F^n un vecteur arithmétique unique $(\alpha_1, \ldots, \alpha_n)$ tel que*

(2) $\mathbf{a} = \alpha_1 \mathbf{b}_1 + \ldots + \alpha_n \mathbf{b}_n$.

D é m o n s t r a t i o n. Vu que le système des vecteurs (1) engendre l'espace $\mathscr{V}$, tout vecteur **a** de V peut être représenté sous forme d'une combinaison linéaire des vecteurs du système (1) tel que (2). Cette représentation est unique. En effet, si

$$\mathbf{a} = \beta_1\mathbf{b}_1 + \ldots + \beta_n\mathbf{b}_n \qquad (\beta_i \in F)$$

est une représentation quelconque de **a** en forme d'une combinaison linéaire des vecteurs (1), alors

$$(\alpha_1 - \beta_1)\,\mathbf{b}_1 + \ldots + (\alpha_n - \beta_n)\,\mathbf{b}_n = \mathbf{0}.$$

En vertu de l'indépendance linéaire du système (1) il s'ensuit les égalités

$$\alpha_1 - \beta_1 = 0, \ldots, \alpha_n - \beta_n = 0 \text{ et } \alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n.$$

Par conséquent, le vecteur **a** possède une représentation unique sous forme d'une combinaison linéaire des vecteurs de la base (1). □

DÉFINITION. Soient $\mathbf{b}_1, \ldots, \mathbf{b}_m$ une base fixée de l'espace $\mathscr{V}$, $\mathbf{a} \in V$ et $\mathbf{a} = \alpha_1\mathbf{b}_1 + \ldots + \alpha_n\mathbf{b}_n$, où $\alpha_1, \ldots, \alpha_n \in F$. Les coefficients $\alpha_1, \ldots, \alpha_n$ sont dits *coordonnées du vecteur* **a** *relativement à la base fixée*. Le vecteur $(\alpha_1, \ldots, \alpha_n) \in F^m$ est appelé *ligne de coordonnées*, tandis que le vecteur $\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{bmatrix}$ est dit *colonne de coordonnées du vecteur* **a** *relativement à la base fixée*.

Isomorphisme des espaces vectoriels. On appelle *application de l'espace vectoriel $\mathscr{U}$ dans $\mathscr{V}$* l'application de l'ensemble U dans V.

DÉFINITION. L'application de l'espace vectoriel $\mathscr{U}$ sur l'espace vectoriel $\mathscr{V}$ est appelée *isomorphisme* si elle est injective et satisfait aux conditions de linéarité:

$$f(\mathbf{a} + \mathbf{b}) = f(\mathbf{a}) + f(\mathbf{b}), \qquad f(\lambda\mathbf{a}) = \lambda f(\mathbf{a})$$

pour des **a**, **b** quelconques de U et tout λ de F. Les espaces vectoriels $\mathscr{U}$ et $\mathscr{V}$ sont dits *isomorphes* si l'on est en présence d'un isomorphisme de $\mathscr{U}$ sur $\mathscr{V}$.

En d'autres termes, l'application f de l'espace vectoriel $\mathscr{U}$ et $\mathscr{V}$ est appelée isomorphisme si elle est injective et respecte les opérations principales de l'espace $\mathscr{U}$ considéré comme une algèbre.

La notation $\mathscr{U} \cong \mathscr{V}$ signifie que les espaces vectoriels $\mathscr{U}$ et $\mathscr{V}$ sont isomorphes.

THÉORÈME 4.2. *Soient $\mathscr{V}$ un espace vectoriel à n dimensions sur le corps $\mathscr{F}$ et $n > 0$. L'espace $\mathscr{V}$ est alors isomorphe à l'espace vectoriel arithmétique $\mathscr{F}^n$.*

D é m o n s t r a t i o n. Soit

(1) $\mathbf{b}_1, \ldots, \mathbf{b}_n$

une base fixée de l'espace $\mathscr{V}$. Soit

$$f: V \to F^n$$

l'application associant à chaque vecteur **a** de V sa ligne de coordonnées $f(\mathbf{a})$ relativement à la base fixée. Soit $(\gamma_1, \ldots, \gamma_n)$ un vecteur arbitraire de F^n. Le vecteur $\gamma_1\mathbf{b}_1 + \ldots + \gamma_n\mathbf{b}_n$ est son image anticipée dans l'application f. Donc, f est l'application de V sur F^n. En outre, selon le théorème 4.1, pour tous **a**, **b** de V si $f(\mathbf{a}) = f(\mathbf{b})$, alors $\mathbf{a} = \mathbf{b}$. Par conséquent, f est une application injective de V sur F^n. L'application f satisfait aux conditions de linéarité. En effet, si $\mathbf{a} = \alpha_1\mathbf{b}_1 + \ldots + \alpha_n\mathbf{b}_n$, $\mathbf{b} = \beta_1\mathbf{b}_1 + \ldots + \beta_n\mathbf{b}_n$, alors

$$\mathbf{a} + \mathbf{b} = (\alpha_1 + \beta_1)\,\mathbf{b}_1 + \ldots + (\alpha_n + \beta_n)\,\mathbf{b}_n$$

et

$$f(\mathbf{a} + \mathbf{b}) = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n) = \\ = (\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) = f(\mathbf{a}) + f(\mathbf{b}).$$

Ensuite, si $\lambda \in F$, alors $\lambda\mathbf{a} = (\lambda\alpha_1)\,\mathbf{b}_1 + \ldots + (\lambda\alpha_n)\,\mathbf{b}_n$ et

$$f(\lambda\mathbf{a}) = (\lambda\alpha_1, \ldots, \lambda\alpha_n) = \lambda(\alpha_1, \ldots, \alpha_n) = \lambda f(\mathbf{a}).$$

Bref, f satisfait aux conditions de linéarité. Par conséquent, l'application f est un isomorphisme de l'espace $\mathscr{V}$ sur l'espace $\mathscr{F}^n$. □

THÉORÈME 4.3. *Soient $\mathscr{V}$ un espace vectoriel à n dimensions sur le corps $\mathscr{F}$ avec une base fixée et $n > 0$. L'application $f: V \to F^n$ associant à chaque vecteur* **a** *de V sa ligne de coordonnées relativement à la base fixée constitue un isomorphisme de l'espace $\mathscr{V}$ sur l'espace vectoriel arithmétique $\mathscr{F}^n$.*

Ce théorème découle directement du théorème 4.2 et de sa démonstration.

COROLLAIRE 4.4. *Soit $\mathscr{V}$ un espace vectoriel de dimension finie $\neq \{0\}$ dont la base est fixée. Un système de vecteurs de l'espace $\mathscr{V}$ est linéairement dépendant si et seulement si le système des lignes (colonnes) de coordonnées de ces vecteurs relativement à la base fixée est linéairement dépendant.*

COROLLAIRE 4.5. *Soit $\mathscr{V}$ un espace vectoriel de dimension finie à base fixée. Le rang du système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ de l'espace $\mathscr{V}$ est égal à celui de la matrice composée des lignes (colonnes) de coordonnées de ces vecteurs relativement à la base fixée.*

Etudions les propriétés des isomorphismes des espaces vectoriels.

PROPRIÉTÉ 4.1. *Si f est un isomorphisme de l'espace vectoriel $\mathscr{U}$ sur $\mathscr{V}$ et g un isomorphisme de l'espace $\mathscr{V}$ sur $\mathscr{W}$, alors leur composition est un isomorphisme de $\mathscr{U}$ sur $\mathscr{W}$.*

Démonstration. Par hypothèse, gf est une application injective de U sur W. L'application gf satisfait aux conditions de linéarité. En effet, en vertu de la linéarité des applications g et f,

pour tous **a**, **b** de V et tout λ de F, il vient :

$$(gf)(\mathbf{a}+\mathbf{b}) = g(f(\mathbf{a}+\mathbf{b})) = g(f(\mathbf{a})+f(\mathbf{b})) = \\ = g(f(\mathbf{a}))+g(f(\mathbf{b})) = (gf)(\mathbf{a})+(gf)(\mathbf{b}),$$

$$(gf)(\lambda\mathbf{a}) = g(f(\lambda\mathbf{a})) = g(\lambda f(\mathbf{a})) = \lambda g(f(\mathbf{a})) = \lambda(gf)(\mathbf{a}).$$

Par conséquent, gf est un isomorphisme de $\mathcal{U}$ sur $\mathcal{V}$. □

PROPRIÉTÉ 4.2. *Si f est un isomorphisme de l'espace vectoriel $\mathcal{U}$ sur l'espace vectoriel $\mathcal{V}$, alors f^{-1} est un isomorphisme de $\mathcal{V}$ sur $\mathcal{U}$.*

Démonstration. f étant une application injective de U sur V, f^{-1} est une application injective de V sur U. En outre, f^{-1} satisfait aux conditions de linéarité. En effet, en vertu de la linéarité de l'application f pour tout **a** de V et tout λ de F, il vient :

$$f(f^{-1}(\mathbf{a})+f^{-1}(\mathbf{b})) = f(f^{-1}(\mathbf{a}))+f(f^{-1}(\mathbf{b})) = \mathbf{a}+\mathbf{b},$$

$$f(\lambda f^{-1}(\mathbf{a})) = \lambda f(f^{-1}(\mathbf{a})) = \lambda\mathbf{a},$$

d'où

$$f^{-1}(\mathbf{a}+\mathbf{b}) = f^{-1}(\mathbf{a})+f^{-1}(\mathbf{b}), \qquad f^{-1}(\lambda\mathbf{a}) = \lambda f^{-1}(\mathbf{a}).$$

Par conséquent, f^{-1} est un isomorphisme de $\mathcal{V}$ sur $\mathcal{U}$. □

PROPRIÉTÉ 4.3. *La relation d'isomorphisme d'un ensemble d'espaces vectoriels quelconque sur le corps $\mathcal{F}$ est une relation d'équivalence.*

Démonstration. La relation d'isomorphisme est apparemment réflexive. En vertu de la propriété 4.1, elle est transitive. En vertu de la propriété 4.2, la relation d'isomorphisme est symétrique. Donc, la relation d'isomorphisme est une relation d'équivalence.

PROPRIÉTÉ 4.4. *Soient*

(1) $\mathbf{b}_1, \ldots, \mathbf{b}_n$

une base de l'espace vectoriel $\mathcal{U}$ et f un isomorphisme de $\mathcal{U}$ sur l'espace vectoriel $\mathcal{V}$. Le système des vecteurs $f(\mathbf{b}_1), \ldots, f(\mathbf{b}_n)$ est alors une base de l'espace $\mathcal{V}$.

Démonstration. Le système des vecteurs

(2) $f(\mathbf{b}_1), \ldots, f(\mathbf{b}_n)$

est linéairement indépendant. En effet, en vertu de la linéarité de l'application f pour tous $\lambda_1, \ldots, \lambda_n$ de F de l'égalité

$$\lambda_1 f(\mathbf{b}_1)+\ldots+\lambda_n f(\mathbf{b}_n) = \mathbf{0}',$$

où $\mathbf{0}'$ est un vecteur zéro de l'espace $\mathcal{V}$, s'ensuivent les égalités

$$f(\lambda_1\mathbf{b}_1+\ldots+\lambda_n\mathbf{b}_n) = \mathbf{0}' = f(\mathbf{0}).$$

Comme l'application f est injective de la dernière égalité il s'ensuit que

(3) $\lambda_1\mathbf{b}_1+\ldots+\lambda_n\mathbf{b}_n = \mathbf{0}.$

Le système (1) étant linéairement indépendant, de (3) dérivent les égalités $\lambda_1 = 0, \ldots, \lambda_n = 0$.

En outre, le système (1) engendre l'espace $\mathcal{V}$. En effet, si $\mathbf{c} \in V$, alors le vecteur $f^{-1}(\mathbf{c}) \in U$ et on peut le représenter sous la forme

$$(4) \quad f^{-1}(\mathbf{c}) = \gamma_1 \mathbf{b}_1 + \ldots + \gamma_n \mathbf{b}_n \qquad (\gamma_1, \ldots, \gamma_n \in F),$$

vu que le système (1) est la base de l'espace $\mathcal{U}$. En vertu de la linéarité de l'application f de (4) s'ensuivent les égalités

$$\mathbf{c} = f(\gamma_1 \mathbf{b}_1 + \ldots + \gamma_n \mathbf{b}_n) = \gamma_1 f(\mathbf{b}_1) + \ldots + \gamma_n f(\mathbf{b}_n).$$

Par conséquent, le système (2) engendre l'espace $\mathcal{V}$ et est sa base.

THÉORÈME 4.6. *Soient $\mathcal{U}$ et $\mathcal{V}$ des espaces vectoriels de dimension finie sur le corps $\mathcal{F}$. Les espaces $\mathcal{U}$ et $\mathcal{V}$ sont isomorphes si et seulement si leurs dimensions sont identiques.*

Démonstration. Supposons que $\mathcal{U} \cong \mathcal{V}$. Si l'un de ces espaces est égal à $\{0\}$, l'autre est également égal à $\{0\}$, c'est-à-dire que $\dim \mathcal{U} = \dim \mathcal{V} = 0$. Supposons maintenant que $\mathcal{U}$ et $\mathcal{V}$ sont des espaces $\neq \{0\}$. Alors, en vertu de la propriété 4.4, le nombre d'éléments de la base de l'espace $\mathcal{U}$ vaut celui de la base de l'espace $\mathcal{V}$ (les dimensions de ces espaces sont identiques).

Posons à présent que $\dim \mathcal{U} = \dim \mathcal{V} = n$. Si $n = 0$ les espaces $\mathcal{U}$, $\mathcal{V} = \{0\}$ et sont donc isomorphes. Mais si $n > 0$, alors, selon le théorème 4.2, $\mathcal{U} \cong \mathcal{F}^n$ et $\mathcal{F}^n \cong \mathcal{V}$. Il s'ensuit, en vertu de la transitivité de l'isomorphisme, que les espaces vectoriels $\mathcal{U}$ et $\mathcal{V}$ sont isomorphes. □

Exercices

1. Soient $\mathcal{U}$ et $\mathcal{V}$ des espaces vectoriels de dimension finie sur le corps $\mathcal{F}$. Montrer qu'il existe un monomorphisme de l'espace $\mathcal{U}$ dans $\mathcal{V}$ si et seulement si $\dim \mathcal{U} \leqslant \dim \mathcal{V}$.
2. Soient $\mathcal{U}$ et $\mathcal{V}$ des espaces vectoriels de dimension finie sur le corps $\mathcal{F}$. Démontrer qu'il existe un épimorphisme de l'espace $\mathcal{U}$ sur $\mathcal{V}$ si et seulement si $\dim \mathcal{U} \geqslant \dim \mathcal{V}$.
3. Soient $\mathcal{U}$ et $\mathcal{V}$ des espaces vectoriels à n dimensions sur un corps fini $\mathcal{F}$ composé de m éléments. Combien y a-t-il d'isomorphismes de l'espace $\mathcal{U}$ sur l'espace $\mathcal{V}$?
4. Donner un exemple d'espace vectoriel sur le corps $\mathcal{F}$ qui ne soit pas de dimension finie.
5. Soit $\mathcal{W}$ un espace vectoriel sur le corps $\mathcal{F}$ de dimension non finie. Montrer qu'il existe un monomorphisme de tout espace vectoriel de dimension finie $\mathcal{V}$ sur le corps $\mathcal{F}$ de l'espace $\mathcal{W}$.

§ 5. Espaces vectoriels à multiplication scalaire

Multiplication scalaire dans un espace vectoriel. Soient $\mathcal{V}$ un espace vectoriel sur le corps $\mathcal{F}$, V l'ensemble de base de l'espace $\mathcal{V}$ et F l'ensemble de base du corps $\mathcal{F}$ appelé *ensemble des scalaires.*

DÉFINITION. On appelle *multiplication scalaire dans l'espace $\mathcal{V}$* une application $V \times V \to F$ associant à chaque couple d'éléments

a, **b** de V un scalaire noté $\mathbf{a}\cdot\mathbf{b}$ et satisfaisant aux conditions:

(1) $\mathbf{a}\cdot\mathbf{b} = \mathbf{b}\cdot\mathbf{a}$ pour tous **a**, **b** de V;

(2) $(\alpha\mathbf{a} + \beta\mathbf{b})\cdot\mathbf{c} = \alpha(\mathbf{a}\cdot\mathbf{c}) + \beta(\mathbf{b}\cdot\mathbf{c})$ pour tous **a**, **b** de V et α, β de F.

Le scalaire $\mathbf{a}\cdot\mathbf{b}$ est appelé *produit scalaire* des vecteurs **a** et **b**.

DÉFINITION. Une multiplication scalaire dans l'espace $\mathscr{V}$ est dite *non dégénérée* si $\mathbf{a}\cdot\mathbf{a} \neq 0$ pour tout vecteur **a** de V non nul. Une multiplication scalaire dans l'espace $\mathscr{V}$ est dite *nulle* si $\mathbf{a}\cdot\mathbf{b} = 0$ pour tous **a**, **b** de V.

PROPOSITION 5.1. *Si $\mathscr{V}$ est un espace vectoriel avec multiplication scalaire, alors* $\mathbf{a}\cdot\mathbf{0} = 0$ *pour tout* **a** *de* V.

Démonstration. En vertu de la condition (2), $\mathbf{a}\cdot\mathbf{0} = \mathbf{a}\cdot(\mathbf{0} + \mathbf{0}) = \mathbf{a}\cdot\mathbf{0} + \mathbf{a}\cdot\mathbf{0}$ et, par suite, $\mathbf{a}\cdot\mathbf{0} + \mathbf{a}\cdot\mathbf{0} = \mathbf{a}\cdot\mathbf{0} + 0$. En vertu de la règle de simplification, il s'ensuit que $\mathbf{a}\cdot\mathbf{0} = 0$. □

Remarquons que dans tout espace vectoriel de dimension finie $\neq \{\mathbf{0}\}$ la multiplication scalaire peut être introduite de manières diverses.

Soit $\mathscr{V}$ un espace vectoriel avec multiplication scalaire

(3) $V \times V \to F$,

satisfaisant aux conditions (1), (2) de la définition. Si $\mathscr{L}$ est un sous-espace de l'espace $\mathscr{V}$, alors l'application (3) induit l application $L \times L \to F$ qui satisfait également sur L aux conditions (1), (2). Aussi le produit vectoriel $\mathscr{L}$ peut-il également être considéré comme un espace vectoriel avec multiplication scalaire.

Système de vecteurs orthogonal. Soit $\mathscr{V}$ un espace vectoriel (sur le corps $\mathscr{F}$) avec multiplication scalaire.

DÉFINITION. Les vecteurs **a**, **b** de V sont dits *orthogonaux* ou *mutuellement orthogonaux* si leur produit scalaire est nul.

La notation $\mathbf{a} \perp \mathbf{b}$ traduit que $\mathbf{a}\cdot\mathbf{b} = 0$.

DÉFINITION. Un système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ de l'espace $\mathscr{V}$ est dit *orthogonal* si sont orthogonaux entre eux deux quelconques des vecteurs du système. Un système comportant un seul vecteur non nul est considéré comme orthogonal. Un système de vecteurs orthogonal constituant la base de l'espace $\mathscr{V}$ est appelé *base orthogonale de l'espace*.

THÉORÈME 5.2. *Soit $\mathscr{V}$ un espace vectoriel avec multiplication scalaire non dégénérée. Le système orthogonal des vecteurs non nuls de l'espace $\mathscr{V}$ est linéairement indépendant.*

Démonstration. Soit

(1) $\mathbf{a}_1, \ldots, \mathbf{a}_m$

un système orthogonal des vecteurs non nuls de l'espace $\mathscr{V}$. Montrons que pour tous scalaires $\lambda_1, \ldots, \lambda_m$ (de F) de l'égalité

(2) $\lambda_1\mathbf{a}_1 + \ldots + \lambda_m\mathbf{a}_m = \mathbf{0}$

se déduit l'égalité à zéro de tous les coefficients. Multiplions les deux membres de l'égalité (2) par le vecteur $\mathbf{a}_k$, $k \in \{1, \ldots, m\}$ et l'on obtient

$$\lambda_1 (\mathbf{a}_1\mathbf{a}_k) + \ldots + \lambda_k (\mathbf{a}_k\mathbf{a}_k) + \ldots + \lambda_m (\mathbf{a}_m\mathbf{a}_k) = 0.$$

En vertu de l'orthogonalité du système (1), on en déduit l'égalité

(3) $\lambda_k (\mathbf{a}_k \cdot \mathbf{a}_k) = 0.$

Vu que par hypothèse, $\mathbf{a}_k \neq 0$ et la multiplication scalaire dans $\mathscr{V}$ n'est pas dégénérée, on a $\mathbf{a}_k\mathbf{a}_k \neq 0$. Donc, de (3) découle l'égalité

$$\lambda_k = 0 \quad \text{pour} \quad k = 1, \ldots, m.$$

Par conséquent, le système des vecteurs (1) est linéairement indépendant. □

COROLLAIRE 5.3. *Si $\mathscr{V}$ est un espace vectoriel à n dimensions $\neq \{\mathbf{0}\}$ avec multiplication scalaire non dégénérée, alors tout système orthogonal de l'espace de n vecteurs non nuls constitue la base orthogonale de l'espace $\mathscr{V}$.*

Procédé d'orthogonalisation. Le principe du procédé d'orthogonalisation ressort de la démonstration du théorème.

THÉORÈME 5.4. *Soit $\mathscr{V}$ un espace vectoriel de dimension finie avec multiplication scalaire non dégénérée. Un système orthogonal de vecteurs non nuls ne constituant pas la base de l'espace peut être complété jusqu'à la base orthogonale de l'espace.*

Démonstration. Soient $\dim \mathscr{V} = n > 1$ et

(1) $\mathbf{b}_1, \ldots, \mathbf{b}_m$

un système orthogonal de vecteurs non nuls de l'espace $\mathscr{V}$ ne constituant pas une base de l'espace, c'est-à-dire $m < n$. Selon le théorème 3.6, le système (1) peut être complété jusqu'à la base. Soit

(2) $\mathbf{b}_1, \ldots, \mathbf{b}_m, \quad \mathbf{c}_{m+1}, \ldots, \mathbf{c}_n$

la base de l'espace $\mathscr{V}$. Posons

(3) $\mathbf{b}_{m+1} = \mathbf{c}_{m+1} - \lambda_1\mathbf{b}_1 - \ldots - \lambda_m\mathbf{b}_m$

et cherchons pour quelles valeurs des scalaires $\lambda_1, \ldots, \lambda_m$ le vecteur $\mathbf{b}_{m+1}$ est orthogonal à tous les vecteurs du système de départ (1), c'est-à-dire satisfait aux conditions

(4) $\mathbf{b}_{m+1}\mathbf{b}_i = 0 \qquad (i = 1, \ldots, m).$

En vertu de (3) et de l'orthogonalité du système (1), ces conditions peuvent être écrites sous la forme

$$\mathbf{c}_{m+1}\mathbf{b}_i - \lambda_i (\mathbf{b}_i\mathbf{b}_i) = 0.$$

Vu que $\mathbf{b}_i \neq 0$ et $\mathbf{b}_i \cdot \mathbf{b}_i \neq 0$, ces conditions s'écrivent sous la forme

$$\lambda_i = \frac{\mathbf{c}_{m+1}\mathbf{b}_i}{\mathbf{b}_i\mathbf{b}_i} \qquad (i = 1, \ldots, m).$$

Avec un tel choix des coefficients λ_i dans l'égalité (3), le vecteur $\mathbf{b}_{m+1}$ satisfait aux conditions (4), c'est-à-dire est orthogonal à chaque vecteur du système (1). Il s'ensuit de (3), en vertu de l'indépendance linéaire du système $\mathbf{b}_1, \ldots, \mathbf{b}_m, \mathbf{b}_{m+1}$, que $\mathbf{b}_{m+1} \neq 0$. Par conséquent, $\mathbf{b}_1, \ldots, \mathbf{b}_m, \mathbf{b}_{m+1}$ est le système orthogonal des vecteurs non nuls. Si $m + 1 < n$, on obtient de façon analogue le vecteur non nul $\mathbf{b}_{m+2}$ orthogonal aux vecteurs $\mathbf{b}_1, \ldots, \mathbf{b}_m, \mathbf{b}_{m+1}$. En poursuivant ce procédé dit *procédé d'orthogonalisation* du système (2) on aboutit au système orthogonal $\mathbf{b}_1, \ldots, \mathbf{b}_m, \mathbf{b}_{m+1}, \ldots, \mathbf{b}_n$ des vecteurs non nuls de l'espace $\mathcal{V}$. Selon le corollaire 5.3, ce système est la base orthogonale de l'espace $\mathcal{V}$ et, par suite, constitue le supplémentaire cherché du système initial (1) jusqu'à la base orthogonale de l'espace $\mathcal{V}$. □

On voit sans peine que l'application du procédé d'orthogonalisation à un système linéairement dépendant des vecteurs non nuls conduit à un système comportant un vecteur nul.

COROLLAIRE 5.5. *Tout espace vectoriel de dimension finie $\neq \{0\}$ avec multiplication scalaire non dégénérée est muni d'une base orthogonale.*

Démonstration. En effet, selon le théorème 3.1, un espace de dimension finie $\neq \{0\}$ possède une base. Soit

(1) $\mathbf{b}_1, \ldots, \mathbf{b}_n$

la base de l'espace $\mathcal{V}$. En posant que $\mathbf{b}_1$ est le système orthogonal de départ et en appliquant au système (1) le procédé d'orthogonalisation, on obtient la base orthogonale de l'espace $\mathcal{V}$.

Supplémentaire orthogonal d'un sous-espace. Soient $\mathcal{V}$ un espace vectoriel avec multiplication scalaire et $M \subset V$. Si le vecteur $\mathbf{a}$ de V est orthogonal à chaque vecteur de M, on le désigne par le symbole $\mathbf{a} \perp M$. Le symbole $M^\perp$ désigne l'ensemble de tous les éléments de l'espace $\mathcal{V}$ orthogonaux à M:

$$M^\perp = \{\mathbf{a} \in V \mid \mathbf{a} \perp M\}.$$

On vérifie aisément que l'ensemble $M^\perp$ n'est pas vide et est fermé dans $\mathcal{V}$, c'est-à-dire fermé par rapport à l'addition et à la multiplication par des scalaires.

DÉFINITION. Un sous-espace de l'espace $\mathcal{V}$ avec ensemble de base $M^\perp$ est dit *orthogonal à l'ensemble M*.

Si $\mathcal{L}$ est un sous-espace de l'espace $\mathcal{V}$, alors le symbole $\mathcal{L}^{\perp}$ désigne le sous-espace à ensemble de base $L^{\perp}$.

DÉFINITION. Un sous-espace $\mathcal{L}^{\perp}$ est dit *orthogonal à $\mathcal{L}$ dans l'espace $\mathcal{V}$* ou *supplémentaire orthogonal de $\mathcal{L}$ dans l'espace $\mathcal{V}$*.

Exemple. Soit $\mathcal{V} = \mathcal{F}^n$ un espace vectoriel arithmétique sur le corps $\mathcal{F}$ avec multiplication scalaire standard. Soient $M = \{\mathbf{a}_1, \ldots, \mathbf{a}_m\} \subset F^n$ et

$$\mathbf{a}_1 = (\alpha_{11}, \ldots, \alpha_{1n}), \ldots, \mathbf{a}_m = (\alpha_{m1}, \ldots, \alpha_{mn}) \qquad (\alpha_{ik} \in F).$$

Considérons un système homogène d'équations linéaires

$$(1) \qquad \begin{array}{l} \alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = 0, \\ \ldots\ldots\ldots\ldots\ldots \\ \alpha_{m1}x_1 + \ldots + \alpha_{mn}x_n = 0 \end{array}$$

sur le corps $\mathcal{F}$. On constate sans peine que l'ensemble $M^{\perp}$ coïncide avec l'ensemble de toutes les solutions du système (1). Soient $\mathcal{L} = \mathcal{L}(\mathbf{a}_1, \ldots, \mathbf{a}_m)$ et $L = L(\mathbf{a}_1, \ldots, \mathbf{a}_m) = L(M)$. On vérifie aisément que chaque vecteur orthogonal à M est orthogonal à toute combinaison linéaire des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$, c'est-à-dire $M^{\perp} \subset L^{\perp}$. Inversement, chaque vecteur de $L^{\perp}$ est orthogonal à M, c'est-à-dire $L^{\perp} \subset M^{\perp}$. Ainsi, $M^{\perp} = L^{\perp}$. Par conséquent, l'espace des solutions du système homogène d'équations linéaires (1) coïncide avec l'espace $\mathcal{L}^{\perp}$.

THÉORÈME 5.6. *Soient $\mathcal{V}$ un espace vectoriel avec multiplication scalaire et $\mathcal{L}$ son sous-espace de dimension finie dans lequel le carré scalaire de tout vecteur non nul est différent de zéro. On a alors $\mathcal{V} = \mathcal{L} \oplus \mathcal{L}^{\perp}$.*

Démonstration. Si $\mathcal{L}$ est un sous-espace $= \{\mathbf{0}\}$, le théorème est apparemment vrai.

Supposons que $\mathcal{L}$ est un espace $\neq \{\mathbf{0}\}$. Démontrons que

$$(1) \qquad L \cap L^{\perp} = \{\mathbf{0}\}.$$

En effet, si $\mathbf{a} \in L \cap L^{\perp}$, alors $\mathbf{a} \cdot \mathbf{a} = 0$. Par hypothèse, $\mathbf{a} \cdot \mathbf{a} \neq 0$ pour $\mathbf{a} \neq \mathbf{0}$. Donc, pour $\mathbf{a} \in L \cap L^{\perp}$ il s'ensuit de $\mathbf{a} \cdot \mathbf{a} = 0$ que $\mathbf{a} = \mathbf{0}$.

Ensuite, démontrons que

$$(2) \qquad \mathcal{V} = \mathcal{L} \oplus \mathcal{L}^{\perp}.$$

Par hypothèse, $\mathcal{L}$ est un espace vectoriel de dimension finie $\neq \{\mathbf{0}\}$ avec multiplication non dégénérée. En vertu du corollaire 5.5, $\mathcal{L}$ est muni d'une base orthogonale. Soit

$$(3) \qquad \mathbf{b}_1, \ldots, \mathbf{b}_m$$

la base orthogonale de l'espace $\mathcal{L}$. Il suffit de montrer que pour tout vecteur $\mathbf{a}$ de L il existe des scalaires $\lambda_1, \ldots, \lambda_m$ et un vecteur

$\mathbf{x}$ tels que

(4) $\mathbf{a} = \lambda_1\mathbf{b}_1 + \ldots + \lambda_m\mathbf{b}_m + \mathbf{x}, \qquad \mathbf{x} \in L^\perp.$

Multiplions les deux membres de l'égalité (4) scalairement par le vecteur $\mathbf{b}_i$, on obtient $\mathbf{a}\cdot\mathbf{b}_i = \lambda_i(\mathbf{b}_i\cdot\mathbf{b}_i)$. Puisque $\mathbf{b}_i\cdot\mathbf{b}_i \neq 0$, il s'ensuit les égalités

(5) $\lambda_i = \dfrac{\mathbf{a}\cdot\mathbf{b}_i}{\mathbf{b}_i\cdot\mathbf{b}_i} \qquad (i = 1, \ldots, m).$

Avec un tel choix des scalaires λ_i le vecteur $\mathbf{x} = \mathbf{a} - \lambda_1\mathbf{b}_1 - \ldots - \lambda_m\mathbf{b}_m$ est orthogonal à chaque vecteur de la base (3), car, en vertu de (4) et (5),

$$\mathbf{x}\mathbf{b}_i = \mathbf{a}\mathbf{b}_i - \lambda_i(\mathbf{b}_i\mathbf{b}_i) = 0 \qquad (i = 1, \ldots, m).$$

Le vecteur $\mathbf{x}$ est donc orthogonal à toute combinaison linéaire des vecteurs $\mathbf{b}_1, \ldots, \mathbf{b}_m$ et, partant, orthogonal à L; donc,

(6) $\mathbf{x} = \mathbf{a} - \lambda_1\mathbf{b}_1 - \ldots - \lambda_m\mathbf{b}_m \in L^\perp.$

Sur la base de (4) et (6) on conclut qu'on est en présence d'une décomposition directe de (2). □

Corollaire 5.7. *Si $\mathscr{L}$ est un sous-espace de dimension finie de l'espace vectoriel $\mathscr{V}$ avec multiplication scalaire non dégénérée, alors $\mathscr{V} = \mathscr{L} \oplus \mathscr{L}^\perp$.*

Corollaire 5.8. *Si $\mathscr{L}$ est un sous-espace de l'espace vectoriel de dimension finie $\mathscr{V}$ avec multiplication scalaire non dégénérée, alors $\mathscr{V} = \mathscr{L} \oplus \mathscr{L}^\perp$.*

Théorème 5.9. *Si $\mathscr{L}$ est un sous-espace d'un espace vectoriel de dimension finie $\mathscr{V}$ avec multiplication scalaire non dégénérée, alors $(\mathscr{L}^\perp)^\perp = \mathscr{L}$.*

On laisse le soin de démontrer ce théorème au lecteur.

Exercices

1. Soit $\mathbf{a}$ un vecteur non nul de l'espace vectoriel $\mathscr{V} = \mathscr{R}^3$ avec multiplication scalaire standard. Quelle est la dimension du sous-espace de l'espace $\mathscr{V}$ orthogonal au vecteur $\mathbf{a}$?

2. Soient $\mathbf{a}, \mathbf{b}$ des vecteurs linéairement indépendants de l'espace $\mathscr{V} = \mathscr{R}^3$ avec multiplication scalaire standard. Chercher la dimension du sous-espace orthogonal aux vecteurs $\mathbf{a}$ et $\mathbf{b}$.

3. Soit $\mathscr{V} = \mathscr{Q}^2$ un espace vectoriel bidimensionnel sur le corps des nombres rationnels avec multiplication scalaire standard. Chercher dans $\mathscr{V}$ le sous-espace $\neq \{0\}$ dans lequel le carré scalaire de tout vecteur est différent de 1.

4. Soit $\mathscr{V}$ un espace vectoriel avec multiplication scalaire non dégénérée. Démontrer que si un vecteur non nul $\mathbf{b}$ est orthogonal aux vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ de l'espace $\mathscr{V}$, alors $\mathbf{b} \notin L(\mathbf{a}_1, \ldots, \mathbf{a}_m)$.

5. Soit $\mathscr{V}$ un espace vectoriel avec multiplication scalaire non dégénérée. Soit $\mathbf{a}_1, \ldots, \mathbf{a}_m$ un système de vecteurs linéairement indépendant de l'espace $\mathscr{V}$. Démontrer que si un vecteur non nul $\mathbf{b}$ est orthogonal aux vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$, le système $\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}$ est alors linéairement indépendant.

6. Soit $\mathcal{L}$ un sous-espace $\neq \{0\}$ d'un espace vectoriel de dimension finie $\mathcal{V}$ avec multiplication scalaire non dégénérée. Soient $\mathbf{a}_1, \ldots, \mathbf{a}_m$ une base orthogonale de l'espace $\mathcal{L}$ et $\mathbf{b}_1, \ldots, \mathbf{b}_s$ une base orthogonale de l'espace $\mathcal{L}^\perp$. Démontrer que $\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}_1, \ldots, \mathbf{b}_s$ est une base orthogonale de l'espace $\mathcal{V}$.

7. Soient $\mathcal{L}$, $\mathcal{U}$ des sous-espaces d'un espace vectoriel de dimension finie $\mathcal{V}$ avec multiplication scalaire non dégénérée. Démontrer que:

(a) $(\mathcal{L}^\perp)^\perp = \mathcal{L}$; (b) $(\mathcal{L}+\mathcal{U})^\perp = \mathcal{L}^\perp \cap \mathcal{U}^\perp$; (c) $(\mathcal{L}\cap\mathcal{U})^\perp = \mathcal{L}^\perp + \mathcal{U}^\perp$.

8. Soient $\mathcal{L}$, $\mathcal{U}$ des sous-espaces de l'espace vectoriel de dimension finie $\mathcal{V}$ avec multiplication scalaire non dégénérée, la dimension de $\mathcal{L}$ étant inférieure à celle de $\mathcal{U}$. Démontrer que dans l'espace $\mathcal{U}$ il y a un vecteur non nul orthogonal au sous-espace $\mathcal{L}$.

9. Soient $\mathcal{L}$, $\mathcal{U}$ des sous-espaces de l'espace vectoriel de dimension finie $\mathcal{V}$ avec multiplication scalaire non dégénérée. Démontrer qu'il existe dans $\mathcal{V}$ un vecteur non nul orthogonal aux sous-espaces $\mathcal{L}$ et $\mathcal{U}$ si $\mathcal{L} + \mathcal{U} \neq \mathcal{V}$.

§ 6. Espaces vectoriels euclidiens

Espace vectoriel euclidien. Soit $\mathcal{V}$ un espace vectoriel avec multiplication scalaire sur le corps $\mathcal{R}$ des nombres réels. Cet espace est également appelé *espace vectoriel réel.*

DÉFINITION. Un espace vectoriel sur le corps $\mathcal{R}$ avec multiplication scalaire définie positive (c'est-à-dire $\mathbf{a}\cdot\mathbf{a} > 0$ pour tout $\mathbf{a} \in V \setminus \{0\}$) est appelé *espace vectoriel euclidien.*

THÉORÈME 6.1. *Un espace vectoriel arithmétique sur le corps $\mathcal{R}$ avec multiplication scalaire standard est euclidien.*

Démonstration. Soient $\mathcal{V} = \mathcal{R}^n$ un espace vectoriel arithmétique avec multiplication scalaire standard et $\mathbf{a} = (\alpha_1, \ldots, \alpha_n)$, $\mathbf{b} = (\beta_1, \ldots, \beta_n)$ des vecteurs de cet espace. Selon la définition de la multiplication scalaire standard, $\mathbf{ab} = \alpha_1\beta_1 + \ldots + \alpha_n\beta_n$. Par conséquent, $\mathbf{aa} = \alpha_1^2 + \ldots + \alpha_n^2$. Et comme $\alpha_1, \ldots, \alpha_n$ sont des nombres réels, on a $\mathbf{aa} > 0$ pour tout vecteur $\mathbf{a}$ non nul de l'espace $\mathcal{V}$. □

DÉFINITION. Un espace vectoriel arithmétique $\mathcal{R}^n$ avec multiplication scalaire standard est dit *espace euclidien standard à n dimensions* et est noté $\mathcal{E}_n$.

Exemple. Considérons l'ensemble V de toutes les fonctions réelles d'une variable réelle x continues sur l'intervalle $[0, 1]$. L'ensemble V par rapport à l'addition et à la multiplication par des nombres réels est un espace (de dimension infinie) vectoriel sur $\mathcal{R}$. La formule $fg = \int_0^1 f(x)\, g(x)\, dx$ définit dans V la multiplication scalaire. On obtient ainsi un espace vectoriel euclidien avec multiplication scalaire.

Norme du vecteur. Soit $\mathcal{V}$ un espace vectoriel euclidien.

DÉFINITION. On appelle *norme du vecteur de l'espace euclidien* la racine carrée arithmétique du carré scalaire du vecteur.

La norme du vecteur est notée $\| \mathbf{a} \|$.

Par définition, $\| \mathbf{a} \| = \sqrt{\mathbf{a}\cdot\mathbf{a}}$. Donc, $\| \mathbf{a} \|^2 = \mathbf{a}\cdot\mathbf{a}$.

DÉFINITION. Le vecteur **a** est dit *normé* si $\| \mathbf{a} \| = 1$.

Le théorème suivant énonce les propriétés fondamentales de la norme d'un vecteur.

THÉORÈME 6.2. *Si* **a**, **b** *sont des vecteurs de l'espace euclidien et* $\lambda \in \mathbf{R}$, *alors*

(1) $\| \mathbf{a} \| \geqslant 0$, *avec* $\| \mathbf{a} \| = 0$ *si et seulement si* $\mathbf{a} = \mathbf{0}$;

(2) $\| \lambda\mathbf{a} \| = | \lambda | \, \| \mathbf{a} \|$;

(3) $| \mathbf{a}\cdot\mathbf{b} | \leqslant \| \mathbf{a} \|\cdot\| \mathbf{b} \|$ (*inégalité de Cauchy-Bouniakovski*);

(4) $\| \mathbf{a} + \mathbf{b} \| \leqslant \| \mathbf{a} \| + \| \mathbf{b} \|$ (*inégalité du triangle*).

Démonstration. La multiplication scalaire dans un espace euclidien est définie positive, c'est-à-dire $\| \mathbf{a} \| = \underset{+}{\sqrt{\mathbf{a}\cdot\mathbf{a}}} > 0$ pour $\mathbf{a} \neq \mathbf{0}$. En outre, $\| \mathbf{a} \| = 0$ pour $\mathbf{a} = \mathbf{0}$.

Selon la définition de la norme

$$\| \lambda\mathbf{a} \| = \underset{+}{\sqrt{(\lambda\mathbf{a})(\lambda\mathbf{a})}} = \underset{+}{\sqrt{\lambda^2(\mathbf{aa})}} = | \lambda | \underset{+}{\sqrt{\mathbf{aa}}} = | \lambda | \cdot \| \mathbf{a} \|,$$

autrement dit, (2) se vérifie.

L'inégalité (3) est vraie si $\mathbf{a} = \mathbf{0}$ ou $\mathbf{b} = \mathbf{0}$. Aussi posera-t-on que **a** et **b** sont des vecteurs non nuls. Pour tous nombres réels α et β on a l'inégalité

$$(\alpha\mathbf{a} - \beta\mathbf{b})(\alpha\mathbf{a} - \beta\mathbf{b}) \geqslant 0.$$

En ouvrant les parenthèses dans le premier membre de l'inégalité $\alpha^2\mathbf{a}^2 - 2\alpha\beta\mathbf{ab} + \beta^2\mathbf{b}^2 \geqslant 0$ et en posant $\alpha = \| \mathbf{b} \|$ et $\beta = \| \mathbf{a} \|$, il vient

$$2(\| \mathbf{a} \|\cdot\| \mathbf{b} \|)^2 - 2\| \mathbf{a} \|\cdot\| \mathbf{b} \|\cdot\mathbf{ab} \geqslant 0,$$

$$\| \mathbf{a} \|\cdot\| \mathbf{b} \|(\| \mathbf{a} \|\cdot\| \mathbf{b} \| - \mathbf{ab}) \geqslant 0.$$

Vu que $\mathbf{a} \neq 0$ et $\mathbf{b} \neq 0$, on a $\| \mathbf{a} \|\cdot\| \mathbf{b} \| \neq 0$, et, par suite,

$$(5) \quad \mathbf{ab} \leqslant \| \mathbf{a} \|\cdot\| \mathbf{b} \|.$$

Substituons dans cette inégalité $-\mathbf{a}$ à **a**:

$$-\mathbf{a}\cdot\mathbf{b} \leqslant \| \mathbf{a} \|\cdot\| \mathbf{b} \|.$$

Sur la base de deux dernières inégalités on conclut qu'on est en présence de l'inégalité (3).

Pour démontrer l'inégalité (4) il suffit de montrer que $\| \mathbf{a} + \mathbf{b} \|^2 \leqslant (\| \mathbf{a} \| + \| \mathbf{b} \|)^2$. On constate aisément que $\| \mathbf{a} + \mathbf{b} \|^2 = (\mathbf{a} + \mathbf{b})(\mathbf{a} + \mathbf{b}) = \| \mathbf{a} \|^2 + \| \mathbf{b} \|^2 + 2\mathbf{ab}$; donc,

$$\| \mathbf{a} + \mathbf{b} \|^2 = (\| \mathbf{a} \| + \| \mathbf{b} \|)^2 + 2(\mathbf{ab} - \| \mathbf{a} \|\cdot\| \mathbf{b} \|).$$

En vertu de (5) le deuxième terme dans le second membre de la dernière égalité est inférieur ou égal à zéro, donc,

$$\| \mathbf{a} + \mathbf{b} \|^2 \leqslant (\| \mathbf{a} \| + \| \mathbf{b} \|)^2;$$

d'où l'on déduit l'inégalité (4). □

Base orthonormée de l'espace euclidien. Une des notions essentielles des espaces euclidiens est celle de base orthonormée.

Définition. Le système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ de l'espace euclidien est dit *orthonormé* s'il est orthogonal, chaque vecteur étant normé. Le système de vecteurs orthonormé constituant la base de l'espace est dit *base orthonormée de l'espace.*

Théorème 6.3. *Un espace vectoriel euclidien de dimension finie $\neq \{0\}$ est muni d'une base orthonormée.*

Démonstration. Soit $\mathcal{V}$ un espace euclidien à n dimensions, $n > 0$. Selon le corollaire 5.5, $\mathcal{V}$ possède une base orthogonale; soit

(1) $\mathbf{b}_1, \ldots, \mathbf{b}_n$

une telle base. Normons le système (1), c'est-à-dire formons le système

$$\mathbf{e}_1 = \| \mathbf{b}_1 \|^{-1} \mathbf{b}_1, \ \ldots, \ \mathbf{e}_n = \| \mathbf{b}_n \|^{-1} \mathbf{b}_n.$$

On voit sans peine que

$$\mathbf{e}_i \mathbf{e}_k = \begin{cases} 1 & \text{si} \quad i = k, \\ 0 & \text{si} \quad i \neq k. \end{cases}$$

Par conséquent, le système $\mathbf{e}_1, \ldots, \mathbf{e}_n$ est une base orthonormée de l'espace $\mathcal{V}$. □

Voyons quelques propriétés d'une base orthonormée.

Propriété 6.1. *Si $\mathcal{V}$ est un espace euclidien à n dimensions $\neq \{0\}$, alors tout système orthonormé de n vecteurs constitue une base orthonormée de l'espace $\mathcal{V}$.*

Cette propriété découle directement du corollaire 5.3.

Propriété 6.2. *Un système orthonormé de vecteurs d'un espace euclidien de dimension finie $\neq \{0\}$ peut être complété jusqu'à la base orthonormée de l'espace.*

Démonstration. Selon le théorème 5.4, un système orthonormé des vecteurs $\mathbf{b}_1, \ldots, \mathbf{b}_m$ ne constituant pas une base peut être complété jusqu'à une base orthogonale

$$\mathbf{b}_1, \ \ldots, \ \mathbf{b}_m, \ \mathbf{b}_{m+1}, \ \ldots, \ \mathbf{b}_n$$

de l'espace. En normant les vecteurs $\mathbf{b}_{m+1}, \ldots, \mathbf{b}_n$ de ce système, c'est-à-dire en substituant $\| \mathbf{b}_i \|^{-1} \cdot \mathbf{b}_i$ à $\mathbf{b}_i$ pour $i = m + 1, \ldots, n$, on obtient une base orthonormée de l'espace. □

PROPRIÉTÉ 6.3. *Si* $\mathbf{e}_1, \ldots, \mathbf{e}_n$ *est une base orthonormée d'un espace euclidien et*

$$\mathbf{a} = \alpha_1\mathbf{e}_1 + \ldots + \alpha_n\mathbf{e}_n, \qquad \mathbf{b} = \beta_1\mathbf{e}_1 + \ldots + \beta_n\mathbf{e}_n$$

sont les vecteurs de l'espace, alors

$$\mathbf{ab} = \alpha_1\beta_1 + \ldots + \alpha_n\beta_n \quad \text{et} \quad \|\mathbf{a}\|^2 = \alpha_1^2 + \ldots + \alpha_n^2.$$

Cette propriété se déduit sans peine de celle de bilinéarité de la multiplication scalaire.

PROPRIÉTÉ 6.4. *Si* $\mathbf{e}_1, \ldots, \mathbf{e}_n$ *est une base orthonormée d'un espace euclidien et* $\mathbf{a} = \alpha_1\mathbf{e}_1 + \ldots + \alpha_n\mathbf{e}_n$, *alors* $\alpha_i = \mathbf{ae}_i$ *pour* $i = 1, \ldots, n$, *c'est-à-dire que les coordonnées du vecteur* **a** *sont ses projections sur les vecteurs de base.*

Démonstration. L'égalité $\alpha_i = \mathbf{ae}_i$ s'obtient de l'égalité $\mathbf{a} = \alpha_1\mathbf{e}_1 + \ldots + \alpha_n\mathbf{e}_n$ après multiplication scalaire par le vecteur $\mathbf{e}_i$. □

PROPRIÉTÉ 6.5. *Si* $\mathcal{L}$ *est un sous-espace de l'espace euclidien de dimension finie* $\mathcal{V}$, *alors* $\mathcal{V} = \mathcal{L} \oplus \mathcal{L}^\perp$ *et* $\dim \mathcal{V} = \dim \mathcal{L} + \dim \mathcal{L}^\perp$.

Cette propriété découle directement du corollaire 5.8 et de la propriété 3.4, car dans un espace euclidien la multiplication scalaire est non dégénérée.

Isomorphismes des espaces euclidiens. Soient $\mathcal{U}$ et $\mathcal{V}$ des espaces euclidiens.

DÉFINITION. L'application f de l'espace euclidien $\mathcal{U}$ sur $\mathcal{V}$ est appelée *isomorphisme* si elle est injective et satisfait aux conditions:

(1) $f(\mathbf{a} + \mathbf{b}) = f(\mathbf{a}) + f(\mathbf{b})$;

(2) $f(\lambda\mathbf{a}) = \lambda f(\mathbf{a})$;

(3) $\mathbf{ab} = f(\mathbf{a}) f(\mathbf{b})$

pour tous **a**, **b** de V et tout scalaire λ de **R**. Les espaces euclidiens sont dits *isomorphes* s'il y a isomorphisme de l'espace euclidien $\mathcal{U}$ sur $\mathcal{V}$.

La notation $\mathcal{U} \cong \mathcal{V}$ signifie que les espaces euclidiens $\mathcal{U}$ et $\mathcal{V}$ sont isomorphes.

Notons les propriétés suivantes des isomorphismes.

PROPRIÉTÉ 6.6. *Une relation d'isomorphisme sur un ensemble quelconque d'espaces euclidiens est une relation d'équivalence.*

Démonstration. On voit sans peine que la relation d'isomorphisme est réflexive.

Profitons des propriétés 4.2 et 4.3 des isomorphismes d'espaces vectoriels. Si f est un isomorphisme de l'espace euclidien $\mathcal{U}$ sur $\mathcal{V}$, alors f^{-1} est bijectif et satisfait aux conditions de linéarité. Ensuite, vu que f satisfait à la condition (3), pour tous **a**, **b**

de V, on a

$$\mathbf{ab} = (ff^{-1})(\mathbf{a})\,(ff^{-1})(\mathbf{b}) = f(f^{-1}(\mathbf{a}))\,f(f^{-1}(\mathbf{b})) = f^{-1}(\mathbf{a})\,f^{-1}(\mathbf{b}),$$

c'est-à-dire l'application f^{-1} satisfait également à la condition (3). f^{-1} est ainsi un isomorphisme de l'espace euclidien $\mathcal{V}$ sur $\mathcal{U}$. Par conséquent, la relation d'isomorphisme des espaces euclidiens est symétrique.

Soient $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$ des espaces euclidiens. Si f est un isomorphisme de $\mathcal{U}$ sur $\mathcal{V}$ et g un isomorphisme de $\mathcal{V}$ sur $\mathcal{W}$, alors, selon la propriété 4.1 des isomorphismes d'espaces vectoriels, la composition gf est une application injective de $\mathcal{U}$ sur $\mathcal{V}$ qui satisfait aux conditions de linéarité. Ensuite, vu que

$$\mathbf{ab} = f(\mathbf{a})\,f(\mathbf{b}), \quad f(\mathbf{a})\,f(\mathbf{b}) = g(f(\mathbf{a}))\,g(f(\mathbf{b})),$$

on a

$$\mathbf{ab} = (gf)(\mathbf{a})\,(gf)(\mathbf{b})$$

pour tous **a**, **b** de U. gf est donc un isomorphisme de l'espace euclidien $\mathcal{U}$ sur $\mathcal{W}$. Par conséquent, la relation d'isomorphisme est transitive. □

PROPRIÉTÉ 6.7. *Soient $\mathcal{U}$, $\mathcal{V}$ des espaces euclidiens et f un isomorphisme de $\mathcal{U}$ sur $\mathcal{V}$. Si $\mathbf{e}_1, \ldots, \mathbf{e}_n$ est une base orthonormée de l'espace $\mathcal{U}$, alors le système $f(\mathbf{e}_1), \ldots, f(\mathbf{e}_n)$ est une base orthonormée de l'espace $\mathcal{V}$.*

D é m o n s t r a t i o n. Comme f est un isomorphisme, on a $\mathbf{e}_i\mathbf{e}_k = f(\mathbf{e}_i)\,f(\mathbf{e}_k)$. Donc,

$$f(\mathbf{e}_i)\,f(\mathbf{e}_k) = \mathbf{e}_i\mathbf{e}_k = \begin{cases} 1 & \text{si} \quad i = k, \\ 0 & \text{si} \quad i \neq k. \end{cases}$$

Le système $f(\mathbf{e}_1), \ldots, f(\mathbf{e}_n)$ est ainsi orthonormé. En outre, selon la propriété 4.4 des isomorphismes des espaces vectoriels, le système $f(\mathbf{e}_1), \ldots, f(\mathbf{e}_n)$ est la base de l'espace $\mathcal{V}$. □

THÉORÈME 6.4. *Tout espace euclidien $\neq \{0\}$ de dimension n est isomorphe à un espace euclidien de dimension n standard.*

D é m o n s t r a t i o n. Soient $\mathcal{V}$ un espace euclidien à n dimensions et $\mathbf{e}_1, \ldots, \mathbf{e}_n$ sa base orthonormée fixée. Soit $\mathcal{E}_n$ un espace euclidien standard à n dimensions. Selon le théorème 4.3 l'application $f\colon V \to \mathbf{R}^n$ associant à chaque vecteur $\mathbf{x} = \xi_1\mathbf{e}_1 + \ldots + \xi_n\mathbf{e}_n$ de V sa ligne de coordonnées $(\xi_1, \ldots, \xi_n)$ est injective et satisfait aux conditions de linéarité. De plus, si $\mathbf{y} = \eta_1\mathbf{e}_1 + \ldots + \eta_n\mathbf{e}_n$, alors

$$\mathbf{xy} = \xi_1\eta_1 + \ldots + \xi_n\eta_n = (\xi_1, \ldots, \xi_n)\,(\eta_1, \ldots, \eta_n) = f(\mathbf{x})\,f(\mathbf{y}).$$

Donc, f est un isomorphisme de l'espace euclidien $\mathcal{V}$ sur l'espace euclidien standard $\mathcal{E}_n$. □

17—01762

THÉORÈME 6.5. *Deux espaces euclidiens de dimension finie sont isomorphes si et seulement si leurs dimensions sont les mêmes.*

Démonstration. Soient $\mathcal{U}$ et $\mathcal{V}$ des espaces euclidiens de dimension finie. Si les espaces $\mathcal{U}$ et $\mathcal{V}$ sont isomorphes, alors on a, selon le théorème 4.6, $\dim \mathcal{U} = \dim \mathcal{V}$.

Admettons maintenant que $\dim \mathcal{U} = \dim \mathcal{V} = n$. Si $n = 0$, les espaces $\mathcal{U}$ et $\mathcal{V}$ sont alors $= \{0\}$ et, partant, isomorphes. Mais si $n > 0$, alors, selon le théorème 6.4, $\mathcal{U} \cong \mathcal{E}_n$ et $\mathcal{E}_n \cong \mathcal{V}$. En vertu de la transitivité de l'isomorphisme, il s'ensuit que les espaces euclidiens $\mathcal{U}$ et $\mathcal{V}$ sont isomorphes. □

Exercices

1. Soient **a**, **b** des vecteurs d'un espace euclidien orthogonaux entre eux. Montrer que $\| \mathbf{a} + \mathbf{b} \|^2 = \| \mathbf{a} \|^2 + \| \mathbf{b} \|^2$.

2. Montrer que pour tous vecteurs **a**, **b** de l'espace euclidien $\| \mathbf{a} + \mathbf{b} \|^2 + \| \mathbf{a} - \mathbf{b} \|^2 = 2 (\| \mathbf{a} \|^2 + \| \mathbf{b} \|^2)$.

3. Soient **a**, **b** des vecteurs de l'espace euclidien tels que $\| \mathbf{a} \| = \| \mathbf{b} \|$. Démontrer que les vecteurs $\mathbf{a} - \mathbf{b}$ et $\mathbf{a} + \mathbf{b}$ sont orthogonaux entre eux.

4. Démontrer que pour tous vecteurs **a**, **b** de l'espace euclidien $| \, \| \mathbf{a} \| - \| \mathbf{b} \| \, | \leqslant \| \mathbf{a} \pm \mathbf{b} \|$.

5. Soient **a**, **b** des vecteurs non nuls de l'espace euclidien. Chercher le vecteur de la forme $\mathbf{a} + \lambda \mathbf{b}$, où $\lambda \in \mathbf{R}$, possédant la plus petite norme et montrer que ce vecteur est orthogonal au vecteur **a**.

6. Soient **a**, **b** des vecteurs linéairement indépendants d'un espace euclidien tridimensionnel $\mathcal{V}$. Démontrer que dans l'espace $\mathcal{V}$ il n'existe que deux vecteurs de norme unitaire qui soient orthogonaux aux vecteurs **a** et **b**.

7. Soit $\mathcal{V} = \mathbf{Q}^2$ un espace vectoriel bidimensionnel sur le corps des nombres rationnels avec multiplication scalaire standard. Chercher dans $\mathcal{V}$ un sous-espace $\neq \{0\}$ dans lequel le carré scalaire d'un vecteur quelconque est différent de 1.

8. Soient **a**, **b** des vecteurs linéairement indépendants de l'espace euclidien $\mathcal{V}$ à n dimensions. Chercher la dimension du sous-espace de l'espace $\mathcal{V}$ orthogonal aux vecteurs **a** et **b**.

9. Soient $\mathcal{U}$ un sous-espace de l'espace euclidien $\mathcal{V}$ à n dimensions et $\mathcal{U}^{\perp}$ son supplémentaire orthogonal. Soient $\mathbf{a}_1, \ldots, \mathbf{a}_s$ une base orthonormée de l'espace $\mathcal{U}$ et $\mathbf{b}_1, \ldots, \mathbf{b}_{n-s}$ une base orthonormée de l'espace $\mathcal{U}^{\perp}$. Démontrer que $\mathbf{a}_1, \ldots, \mathbf{a}_s, \mathbf{b}_1, \ldots, \mathbf{b}_{n-s}$ est une base orthonormée de l'espace $\mathcal{V}$.

10. Soient **a**, **b** des vecteurs de l'espace vectoriel euclidien. Démontrer que $| \mathbf{a} \cdot \mathbf{b} | = \| \mathbf{a} \| \cdot \| \mathbf{b} \|$ si et seulement si les vecteurs **a** et **b** sont linéairement dépendants.

11. Soient $\mathbf{a}_1, \ldots, \mathbf{a}_m$ un système orthonormé de vecteurs de l'espace euclidien $\mathcal{V}$. Posons que pour chaque vecteur **c** de l'espace $\mathcal{V}$ $\| \mathbf{c} \|^2 = (\mathbf{a}_1 \mathbf{c})^2 + \ldots + (\mathbf{a}_m \mathbf{c})^2$. Démontrer que le système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ est une base de l'espace $\mathcal{V}$.

12. Soient $\mathcal{L}$, $\mathcal{U}$ des sous-espaces de l'espace vectoriel euclidien de dimension finie. Démontrer que:

(a) $(\mathcal{L}^{\perp})^{\perp} = \mathcal{L}$; (b) $(\mathcal{L} + \mathcal{U})^{\perp} = \mathcal{L}^{\perp} \cap \mathcal{U}^{\perp}$; (c) $(\mathcal{L} \cap \mathcal{U})^{\perp} = \mathcal{L}^{\perp} + \mathcal{U}^{\perp}$.

CHAPITRE VIII

OPÉRATEURS LINÉAIRES

§ 1. Applications linéaires

Applications et opérateurs linéaires. Passons à l'étude des homomorphismes des espaces vectoriels; ils sont également nommés applications linéaires.

DÉFINITION. Soient $\mathcal{U}$ et $\mathcal{V}$ des espaces vectoriels sur le corps $\mathcal{F}$. Une application $f: \mathcal{U} \to \mathcal{V}$ est appelée *application linéaire* ou *homomorphisme* si cette dernière satisfait aux conditions de linéarité, c'est-à-dire pour tous $\mathbf{a}$, $\mathbf{b} \in V$ et tout $\lambda \in F$ sont satisfaites les conditions

$$f(\mathbf{a} + \mathbf{b}) = f(\mathbf{a}) + f(\mathbf{b}), \quad f(\lambda\mathbf{a}) = \lambda f(\mathbf{a}).$$

Si une application linéaire de $\mathcal{U}$ sur $\mathcal{V}$ est injective, elle s'appelle alors *isomorphisme* ou *application isomorphe* de $\mathcal{U}$ sur $\mathcal{V}$.

Un ensemble de toutes les applications linéaires (homomorphismes) de l'espace $\mathcal{U}$ dans l'espace $\mathcal{V}$ sera noté Hom $(\mathcal{U}, \mathcal{V})$.

Une application linéaire de l'espace vectoriel $\mathcal{V}$ dans lui-même est appelée *opérateur linéaire de l'espace* $\mathcal{V}$. Un ensemble de tous les opérateurs linéaires de l'espace $\mathcal{V}$ est noté Hom $(\mathcal{V}, \mathcal{V})$.

Soit φ une application linéaire de l'espace vectoriel $\mathcal{U}$ sur l'espace vectoriel $\mathcal{V}$. Alors, pour tous vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_n$ de $\mathcal{U}$ et tous scalaires $\lambda_1, \ldots, \lambda_m \in F$, on a

$$(1) \quad \varphi(\lambda_1\mathbf{a}_1 + \ldots + \lambda_m\mathbf{a}_m) = \lambda_1\varphi(\mathbf{a}_1) + \ldots + \lambda_m\varphi(\mathbf{a}_m).$$

La démonstration est effectuée par récurrence sur m. Si $m = 1$, en vertu de la linéarité de l'application φ, on a $\varphi(\lambda_1\mathbf{a}_1) = \lambda_1\varphi(\mathbf{a}_1)$. Posons que la proposition est vraie pour $m - 1$ vecteurs. Alors, en utilisant l'égalité

$$\lambda_1\mathbf{a}_1 + \ldots + \lambda_{m-1}\mathbf{a}_{m-1} + \lambda_m\mathbf{a}_m = (\lambda_1\mathbf{a}_1 + \ldots + \lambda_{m-1}\mathbf{a}_{m-1}) + \lambda_m\mathbf{a}_m,$$

il vient

$$\varphi(\lambda_1\mathbf{a}_1 + \ldots + \lambda_m\mathbf{a}_m) = \varphi(\lambda_1\mathbf{a}_1 + \ldots + \lambda_{m-1}\mathbf{a}_{m-1}) + \varphi(\lambda_m\mathbf{a}_m).$$

Selon l'hypothèse de récurrence

$$\varphi(\lambda_1 \mathbf{a}_1 + \ldots + \lambda_{m-1}\mathbf{a}_{m-1}) = \lambda_1\varphi(\mathbf{a}_1) + \ldots + \lambda_{m-1}\varphi(\mathbf{a}_{m-1}).$$

En outre, $\varphi(\lambda_m \mathbf{a}_m) = \lambda_m \varphi(\mathbf{a}_m)$. Par conséquent, l'égalité (1) est vérifiée. □

Exemples. 1. Soit $\mathscr{V}$ un espace vectoriel. L'application $\varepsilon: \mathscr{V} \to \mathscr{V}$ associant à chaque vecteur $\mathbf{x}$ de V le vecteur lui-même, c'est-à-dire $\varepsilon(\mathbf{x}) = \mathbf{x}$ est un opérateur linéaire. Il est appelé *opérateur identique* ou *unitaire de l'espace*.

2. Soient $\mathscr{V}$ un espace vectoriel sur le corps $\mathscr{F}$ et λ un élément fixé du corps. L'application $\lambda\varepsilon: \mathscr{V} \to \mathscr{V}$ associant au vecteur $\mathbf{x}$ le vecteur $\lambda\mathbf{x}$ est un opérateur linéaire de l'espace $\mathscr{V}$. On l'appelle *opérateur d'homothétie* de coefficient λ. L'opérateur d'homothétie de coefficient $\lambda = 0$ est dit *opérateur zéro*. L'opérateur d'homothétie de coefficient $\lambda = 1$ est un opérateur identique.

3. Soit $\mathscr{V} = \mathscr{L} \oplus \mathscr{U}$. Tout élément $\mathbf{x}$ de $\mathscr{V}$ sera représenté de façon unique sous forme de $\mathbf{x} = \mathbf{l} + \mathbf{u}$, où $\mathbf{l} \in L$ et $\mathbf{u} \in U$. L'application $\mathscr{V} \to \mathscr{V}$ associant au vecteur $\mathbf{x}$ sa composante $\mathbf{l}$ dans le terme direct de $\mathscr{U}$ est un opérateur linéaire de l'espace $\mathscr{V}$. On l'appelle *opérateur projectif*.

4. Soit $\mathscr{V}$ un espace vectoriel (sur $\mathscr{R}$) des fonctions réelles à une variable x définies et indéfiniment dérivables sur l'ensemble $\mathbf{R}$ des nombres réels. L'opérateur $\mathrm{D}: \mathscr{V} \to \mathscr{V}$ associant à chaque élément $f \in V$ sa dérivée $\frac{\mathrm{d}f}{\mathrm{d}x}$ est un opérateur linéaire, car il satisfait aux conditions de linéarité

$$\mathrm{D}(f + g) = \mathrm{D}(f) + \mathrm{D}(g); \quad \mathrm{D}(\lambda f) = \lambda \mathrm{D}(f)$$

pour tous $f, g \in V$ et tout $\lambda \in \mathbf{R}$. Cet opérateur est appelé *opérateur de dérivation*.

5. Soient $\mathscr{V} = \mathscr{F}^n$ un espace arithmétique de vecteurs colonnes de n dimensions et A une matrice carrée $n \times n$ fixée sur le corps $\mathscr{F}$. L'application de l'espace $\mathscr{V}$ dans lui-même associant à chaque vecteur $X \in F^n$ le vecteur AX est un opérateur linéaire de l'espace $\mathscr{V}$.

THÉORÈME 1.1. *Soient $\mathscr{U}$ et $\mathscr{V}$ des espaces vectoriels sur le corps $\mathscr{F}$, $\mathbf{e}_1, \ldots, \mathbf{e}_n$ la base de l'espace $\mathscr{U}$ et $\mathbf{c}_1, \ldots, \mathbf{c}_n$ des vecteurs arbitraires de l'espace $\mathscr{V}$. Il existe alors une application linéaire unique φ de l'espace $\mathscr{U}$ dans l'espace $\mathscr{V}$ satisfaisant aux conditions*

$$(1) \quad \varphi(\mathbf{e}_1) = \mathbf{c}_1, \ldots, \varphi(\mathbf{e}_n) = \mathbf{c}_n.$$

Démonstration. Tout vecteur de l'espace $\mathscr{U}$ peut être représenté sous forme d'une combinaison linéaire des vecteurs de base, c'est-à-dire sous la forme de $\lambda_1\mathbf{e}_1 + \ldots + \lambda_n\mathbf{e}_n$. Notons φ l'application de $\mathscr{U}$ dans $\mathscr{V}$, définie par l'égalité

$$\varphi(\lambda_1\mathbf{e}_1 + \ldots + \lambda_n\mathbf{e}_n) = \lambda_1\mathbf{c}_1 + \ldots + \lambda_n\mathbf{c}_n$$

pour tous $\lambda_1, \ldots, \lambda_n$ de F.

On constate sans peine que l'application φ satisfait aux conditions (1).

L'application φ satisfait aux conditions de linéarité. En effet, si

$$\mathbf{x} = \alpha_1\mathbf{e}_1 + \ldots + \alpha_n\mathbf{e}_n \text{ et } \mathbf{y} = \beta_1\mathbf{e}_1 + \ldots + \beta_n\mathbf{e}_n,$$

alors

$$\mathbf{x} + \mathbf{y} = (\alpha_1 + \beta_1)\,\mathbf{e}_1 + \ldots + (\alpha_n + \beta_n)\,\mathbf{e}_n$$
$$\text{et } \lambda x = \lambda\alpha_1\mathbf{e}_1 + \ldots + \lambda\alpha_n\mathbf{x}_n.$$

Par conséquent, en vertu de la définition de l'application φ,

$$\varphi(\mathbf{x} + \mathbf{y}) = (\alpha_1 + \beta_1)\,\mathbf{c}_1 + \ldots + (\alpha_n + \beta_n)\,\mathbf{c}_n =$$
$$= (\alpha_1\mathbf{c}_1 + \ldots + \alpha_n\mathbf{c}_n) + (\beta_1\mathbf{c}_1 + \ldots + \beta_n\mathbf{c}_n) =$$
$$= \varphi(\mathbf{x}) + \varphi(\mathbf{y});$$
$$\varphi(\lambda\mathbf{x}) = \lambda\alpha_1\mathbf{c}_1 + \ldots + \lambda\alpha_n\mathbf{c}_n = \lambda(\alpha_1\mathbf{c}_1 + \ldots + \alpha_n\mathbf{c}_n) =$$
$$= \lambda\varphi(\mathbf{x}).$$

Posons que ψ est une application linéaire de $\mathcal{U}$ dans $\mathcal{V}$ satisfaisant aux conditions $\psi(\mathbf{e}_1) = \mathbf{c}_1, \ldots, \psi(\mathbf{e}_n) = \mathbf{c}_n$. Alors, pour tout vecteur $\mathbf{x} = \alpha_1\mathbf{e}_1 + \ldots + \alpha_n\mathbf{e}_n$ de l'espace $\mathcal{U}$, il vient

$$\psi(\mathbf{x}) = \alpha_1\psi(\mathbf{e}_1) + \ldots + \alpha_n\psi(\mathbf{e}_n) = \alpha_1\mathbf{c}_1 + \ldots + \alpha_n\mathbf{c}_n =$$
$$= \varphi(\mathbf{x}),$$

c'est-à-dire $\psi = \varphi$. □

COROLLAIRE 1.2. *Soient $\mathcal{U}$ et $\mathcal{V}$ des espaces vectoriels sur $\mathcal{F}$, $\mathbf{e}_1, \ldots, \mathbf{e}_n$ une base de l'espace $\mathcal{U}$; φ et ψ des applications linéaires de $\mathcal{U}$ dans $\mathcal{V}$ telles que $\varphi(\mathbf{e}_k) = \psi(\mathbf{e}_k)$ pour $k = 1, \ldots, n$. Alors, $\varphi = \psi$.*

COROLLAIRE 1.3. *Soient $\mathbf{e}_1, \ldots, \mathbf{e}_n$ une base de l'espace vectoriel $\mathcal{V}$ et $\mathbf{c}_1, \ldots, \mathbf{c}_n$ des vecteurs arbitraires de cet espace. Il existe alors un opérateur linéaire unique φ de l'espace $\mathcal{V}$ satisfaisant aux conditions* (1).

Noyau et image de l'opérateur linéaire. Soit φ l'opérateur linéaire de l'espace vectoriel $\mathcal{V}$. L'ensemble $\{x \in V \mid \varphi(\mathbf{x}) = 0\}$ est noté Ker φ. Autrement dit, l'ensemble Ker φ est une image inverse du vecteur nul dans l'application φ, Ker $\varphi = \varphi^{-1}(0)$. En vertu de la linéarité de l'opérateur φ, cet ensemble est fermé par rapport à l'addition et à la multiplication par des scalaires. Par conséquent, il existe un sous-espace de l'espace $\mathcal{V}$ avec ensemble de base Ker φ.

DÉFINITION. Un sous-espace de l'espace vectoriel $\mathcal{V}$ avec ensemble de base Ker φ est appelé *noyau de l'opérateur linéaire* φ et noté $\mathcal{K}er$ φ. La dimension du noyau porte le nom de *défaut de l'opérateur* φ, défaut φ = dim $\mathcal{K}er$ φ.

L'ensemble $\{\varphi(\mathbf{x}) \mid \mathbf{x} \in V\}$ est noté Im φ ou $\varphi(V)$. En vertu de la linéarité de l'opérateur φ, cet ensemble est fermé par rapport à l'addition et à la multiplication par des scalaires. Il existe donc un sous-espace de l'espace $\mathcal{V}$ avec ensemble de base Im φ.

DÉFINITION. Un sous-espace de l'espace vectoriel $\mathscr{V}$ avec ensemble de base Im φ est appelé *image de l'opérateur linéaire* φ et noté $\mathscr{I}m\varphi$. La dimension de l'image de l'opérateur φ est appelée *rang de l'opérateur* φ, rang $\varphi = \dim(\mathscr{I}m\varphi)$.

THÉORÈME 1.4. *Soit* φ *un opérateur linéaire d'un espace vectoriel de dimension finie* $\mathscr{V}$. *Alors*

(1) *la somme du rang et du défaut de l'opérateur* φ *vaut* dim $\mathscr{V}$.

Démonstration. Premier cas: Ker $\varphi = \{0\}$. Si $\mathscr{V} = \{0\}$, on voit immédiatement que la conclusion du théorème est vraie. Supposons que $\mathscr{V}$ est un espace $\neq \{0\}$. Soient dim $\mathscr{V} = n$ et $\mathbf{e}_1, \ldots, \mathbf{e}_n$ une base de l'espace $\mathscr{V}$. Alors, le système des vecteurs $\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n)$ engendre l'espace $\mathscr{I}m\varphi$, c'est-à-dire Im $\varphi = L(\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n))$.

Ce système de vecteurs est linéairement indépendant. En effet, si

$$\lambda_1\varphi(\mathbf{e}_1) + \ldots + \lambda_n\varphi(\mathbf{e}_n) = \mathbf{0},$$

alors, en vertu de la linéarité de l'opérateur φ,

$$\varphi(\lambda_1\mathbf{e}_1 + \ldots + \lambda_n\mathbf{e}_n) = \mathbf{0}.$$

Comme Ker $\varphi = \{0\}$, il s'ensuit que

$$\lambda_1\mathbf{e}_1 + \ldots + \lambda_n\mathbf{e}_n = \mathbf{0}$$

et, en vertu de l'indépendance linéaire des vecteurs, $\lambda_1 = 0, \ldots, \lambda_n = 0$. Le système $\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n)$ est ainsi une base de l'espace $\mathscr{I}m\varphi$ et, par suite, le rang φ vaut n. En outre, le défaut φ est égal à zéro. Par conséquent, l'affirmation (1) se vérifie.

Deuxième cas: Ker $\varphi \neq \{0\}$. Posons que défaut $\varphi = r$ et $\mathbf{e}_1, \ldots, \mathbf{e}_r$ est une base du noyau de l'opérateur φ, la base de l'espace $\mathscr{K}er\,\varphi$. Si $r = \dim \mathscr{V}$, alors l'affirmation (1) est apparemment vraie. Admettons que $r < n = \dim \mathscr{V}$. Dans ce cas le système $\mathbf{e}_1, \ldots, \mathbf{e}_r$ peut être complété jusqu'à la base de l'espace $\mathscr{V}$. Soit $\mathbf{e}_1, \ldots, \mathbf{e}_r, \mathbf{e}_{r+1}, \ldots, \mathbf{e}_n$ la base de l'espace $\mathscr{V}$; alors

$$\text{Im}\,\varphi = L(\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n)).$$

Vu que $\varphi(\mathbf{e}_1) = \mathbf{0}, \ldots, \varphi(\mathbf{e}_r) = \mathbf{0}$, on a

$$\text{Im}\,\varphi = L(\varphi(\mathbf{e}_{r+1}), \ldots, \varphi(\mathbf{e}_n)),$$

autrement dit, le système des vecteurs $\varphi(\mathbf{e}_{r+1}), \ldots, \varphi(\mathbf{e}_n)$ engendre l'espace $\mathscr{I}m\varphi$.

Ce système est linéairement indépendant. En effet, si

$$\lambda_{r+1}\varphi(\mathbf{e}_{r+1}) + \ldots + \lambda_n\varphi(\mathbf{e}_n) = \mathbf{0},$$

alors, en vertu de la linéarité de l'opérateur φ,

$$\varphi(\lambda_{r+1}\mathbf{e}_{r+1} + \ldots + \lambda_n\mathbf{e}_n) = \mathbf{0},$$

d'où

$$\lambda_{r+1}\mathbf{e}_{r+1} + \ldots + \lambda_n\mathbf{e}_n \in \operatorname{Ker} \varphi.$$

Puisque $\mathbf{e}_1, \ldots, \mathbf{e}_r$ est une base de l'espace $\mathcal{K}er\ \varphi$, il existe des scalaires $\lambda_1, \ldots, \lambda_r$ tels que

$$\lambda_{r+1}\mathbf{e}_{r+1} + \ldots + \lambda_n\mathbf{e}_n = \lambda_1\mathbf{e}_1 + \ldots + \lambda_r\mathbf{e}_r$$

et, par suite,

$$(-\lambda_1)\,\mathbf{e}_1 + \ldots + (-\lambda_r)\,\mathbf{e}_r + \lambda_{r+1}\mathbf{e}_{r+1} + \ldots + \lambda_n\mathbf{e}_n = 0.$$

En vertu de l'indépendance linéaire des vecteurs $\mathbf{e}_1, \ldots, \mathbf{e}_n$ il s'ensuit que tous les coefficients du second membre de l'égalité sont nuls et, en particulier, $\lambda_{r+1} = 0, \ldots, \lambda_n = 0$. Le système des vecteurs $\varphi(\mathbf{e}_{r+1}), \ldots, \varphi(\mathbf{e}_n)$ est ainsi une base de l'espace $\mathcal{I}m\varphi$ et le rang φ vaut $n - r$. Par conséquent, l'affirmation (1) est vraie. □

Opérations sur des applications linéaires. Soient $\mathcal{U}$ et $\mathcal{V}$ des espaces vectoriels sur le corps $\mathcal{F}$, φ, ψ des applications linéaires de $\mathcal{U}$ dans $\mathcal{V}$. La somme $\varphi + \psi$ est définie comme une application de $\mathcal{U}$ dans $\mathcal{V}$ qui associe à l'élément $\mathbf{x}$ $\mathcal{U}$ de l'élément $\varphi(\mathbf{x}) + \psi(\mathbf{x})$ de $\mathcal{V}$, c'est-à--dire

$$(\varphi + \psi)(\mathbf{x}) = \varphi(\mathbf{x}) + \psi(\mathbf{x}).$$

Le produit du scalaire $\lambda \in F$ et de l'application φ est défini comme application de $\mathcal{U}$ dans $\mathcal{V}$ associant à l'élément $\mathbf{x} \in \mathcal{U}$ l'élément $\lambda\varphi(\mathbf{x})$ de l'espace $\mathcal{V}$, c'est-à-dire $(\lambda\varphi)(\mathbf{x}) = \lambda\varphi(\mathbf{x})$.

PROPOSITION 1.5. *Soient φ et ψ des applications linéaires de l'espace vectoriel $\mathcal{U}$ dans l'espace vectoriel $\mathcal{V}$ et $\lambda \in F$. Alors $\varphi + \psi$ et $\lambda\varphi$ sont des applications linéaires de $\mathcal{U}$ dans $\mathcal{V}$.*

D é m o n s t r a t i o n. La somme $\varphi + \psi$ satisfait aux conditions de linéarité. En effet, pour tous $\mathbf{a}, \mathbf{b} \in U$ et tout $\lambda \in F$, on a:

$$(\varphi + \psi)(\mathbf{a} + \mathbf{b}) = \varphi(\mathbf{a} + \mathbf{b}) + \psi(\mathbf{a} + \mathbf{b}) = \varphi(\mathbf{a}) + \varphi(\mathbf{b}) + \\ + \psi(\mathbf{a}) + \psi(\mathbf{b}) = \varphi(\mathbf{a}) + \psi(\mathbf{a}) + \varphi(\mathbf{b}) + \psi(\mathbf{b}) = \\ = (\varphi + \psi)(\mathbf{a}) + (\varphi + \psi)(\mathbf{b});$$

$$(\varphi + \psi)(\lambda\mathbf{a}) = \varphi(\lambda\mathbf{a}) + \psi(\lambda\mathbf{a}) = \lambda\varphi(\mathbf{a}) + \lambda\psi(\mathbf{a}) = \\ = \lambda(\varphi(\mathbf{a}) + \psi(\mathbf{a})) = \lambda((\varphi + \psi)(\mathbf{a})).$$

Ainsi, $\varphi + \psi$ est une application linéaire de $\mathcal{U}$ dans $\mathcal{V}$.

Le produit $\lambda\varphi$ satisfait aux conditions de linéarité. En effet, pour tous $\mathbf{a}, \mathbf{b} \in U$ et tout $\lambda \in F$ on a:

$$(\lambda\varphi)(\mathbf{a} + \mathbf{b}) = \lambda(\varphi(\mathbf{a} + \mathbf{b})) = \lambda(\varphi(\mathbf{a}) + \varphi(\mathbf{b})) = \\ = \lambda\varphi(\mathbf{a}) + \lambda\varphi(\mathbf{b}) = (\lambda\varphi)(\mathbf{a}) + (\lambda\varphi)(\mathbf{b});$$

$$(\lambda\varphi)(\mu\mathbf{a}) = \lambda\varphi(\mu\mathbf{a}) = \lambda(\mu\varphi(\mathbf{a})) = (\lambda\mu)\varphi(\mathbf{a}) = \\ = \mu(\lambda\varphi(\mathbf{a})) = \mu((\lambda\varphi)(\mathbf{a})).$$

Par conséquent, $\lambda\varphi$ est une application linéaire de $\mathcal{U}$ dans $\mathcal{V}$. □

COROLLAIRE 1.6. *L'ensemble* Hom $(\mathcal{U}, \mathcal{V})$ *est fermé par rapport à l'addition et à la multiplication par des scalaires.*

Exercices

1. Soit φ un opérateur linéaire de l'espace vectoriel unidimensionnel $\mathcal{V}$ sur le corps $\mathcal{F}$. Démontrer qu'il existe un scalaire $\lambda \in F$ tel que $\varphi(\mathbf{x}) = \lambda\mathbf{x}$ pour tout vecteur $\mathbf{x} \in V$.

2. Soient φ et ψ des opérateurs linéaires de l'espace vectoriel de dimension finie et $\varphi\psi = 0$. Aura-t-on $\psi\varphi = 0$?

3. Soient φ une application linéaire de l'espace vectoriel $\mathcal{U}$ dans l'espace $\mathcal{V}$ et $\mathbf{b} \in \operatorname{Im}\varphi$. Démontrer que l'ensemble $\varphi^{-1}(\mathbf{b})$ $(\varphi^{-1}(\mathbf{b}) = \{\mathbf{x} \in V \mid \varphi(\mathbf{x}) = \mathbf{b}\})$ est une variété linéaire de l'espace $\mathcal{U}$ de direction $\mathcal{K}er\,\varphi$.

4. Soient φ une application linéaire de l'espace vectoriel $\mathcal{U}$ dans l'espace $\mathcal{V}$ et $\mathbf{a}_1, \ldots, \mathbf{a}_m \in U$. Démontrer que si le système $\varphi(\mathbf{a}_1), \ldots, \varphi(\mathbf{a}_m)$ est linéairement indépendant dans $\mathcal{V}$, le système $\mathbf{a}_1, \ldots, \mathbf{a}_m$ est alors linéairement indépendant dans $\mathcal{U}$.

5. Soit φ une application linéaire injective de l'espace vectoriel $\mathcal{U}$ dans l'espace $\mathcal{V}$. Démontrer que si le système $\mathbf{a}_1, \ldots, \mathbf{a}_m$ est linéairement indépendant dans $\mathcal{U}$, le système $\varphi(\mathbf{a}_1), \ldots, \varphi(\mathbf{a}_m)$ est alors linéairement indépendant dans $\mathcal{V}$.

6. Démontrer que l'application linéaire φ de l'espace vectoriel $\mathcal{U}$ dans l'espace $\mathcal{V}$ est injective si et seulement si $\mathcal{K}er\,\varphi = \{0\}$.

7. Soit φ une application linéaire de l'espace vectoriel $\mathcal{U}$ à n dimensions dans l'espace $\mathcal{V}$ de dimension n. Démontrer que φ est un isomorphisme.

8. Soient φ une application linéaire de l'espace vectoriel $\mathcal{U}$ sur l'espace unidimensionnel $\mathcal{V}$ et $\mathbf{a} \in U \setminus \operatorname{Ker}\varphi$. Démontrer que $\mathcal{U} = \mathcal{K}er\,\varphi \oplus \mathcal{L}(\mathbf{a})$.

9. Soient φ, ψ des opérateurs linéaires de l'espace vectoriel $\mathcal{V}$ tels que $\operatorname{Ker}\varphi = \operatorname{Ker}\psi = \{0\}$. Démontrer que $\operatorname{Ker}(\varphi\psi) = \{0\}$.

10. Soit φ un opérateur linéaire de l'espace vectoriel $\mathcal{V}$ satisfaisant à la condition $\varphi \circ \varphi = \varphi$. Montrer que $\mathcal{V} = \mathcal{K}er\,\varphi \oplus \mathcal{I}m\,\varphi$.

11. Soient $\mathcal{U}$ et $\mathcal{V}$ des espaces vectoriels sur le corps $\mathcal{F}$, l'espace $\mathcal{U}$ étant unidimensionnel. Démontrer que toute application différente de zéro de $\mathcal{U}$ dans $\mathcal{V}$ est injective.

12. Soit $\mathcal{H}om\,(\mathcal{U}, \mathcal{V})$ un espace vectoriel de toutes les applications linéaires de l'espace vectoriel $\mathcal{U}$ de dimension finie dans l'espace de dimension finie $\mathcal{V}$. Démontrer que

(a) si $\dim \mathcal{U} = 1$, alors $\dim(\mathcal{H}om\,(\mathcal{U}, \mathcal{V})) = \dim \mathcal{V}$,

(b) si $\dim \mathcal{V} = 1$, alors $\dim(\mathcal{H}om\,(\mathcal{U}, \mathcal{V})) = \dim \mathcal{U}$.

13. Soient $\mathcal{U}$ et $\mathcal{V}$ des espaces vectoriels de dimension finie dont les dimensions sont m et n. Démontrer que la dimension de l'espace vectoriel $\mathcal{H}om\,(\mathcal{U}, \mathcal{V})$ vaut le produit mn.

14. Soit φ l'application linéaire de l'espace vectoriel de dimension finie $\mathcal{U}$ dans l'espace vectoriel $\mathcal{V}$. Démontrer que

$$\dim(\mathcal{K}er\,\varphi) + \dim(\mathcal{I}m\,\varphi) = \dim \mathcal{U}.$$

15. Soit φ une application linéaire de l'espace vectoriel $\mathcal{U}$ dans l'espace vectoriel de dimension finie $\mathcal{V}$. Soit $\mathbf{a}_1, \ldots, \mathbf{a}_m$ un système de vecteurs de l'espace $\mathcal{U}$ tel que le système $\varphi(\mathbf{a}_1), \ldots, \varphi(\mathbf{a}_m)$ soit une base de l'espace $\mathcal{I}m\,\varphi$. Démontrer que

$$\mathcal{U} = \mathcal{K}er\,\varphi \oplus \mathcal{L}(\mathbf{a}_1, \ldots, \mathbf{a}_m).$$

16. Soit φ un opérateur linéaire de l'espace vectoriel de dimension finie $\mathcal{V}$ sur le corps $\mathcal{F}$. Démontrer que pour un nombre naturel suffisamment grand m les opérateurs linéaires $\varphi, \varphi^2, \ldots, \varphi^m$ sont linéairement dépendants sur le corps $\mathcal{F}$.

§ 2. Représentation des opérateurs linéaires par des matrices

Matrice d'un opérateur linéaire. Soit $\mathcal{V}$ un espace vectoriel de dimension finie sur le corps $\mathcal{F}$,

$$(1) \quad \mathbf{e}_1, \ldots, \mathbf{e}_n$$

étant sa base et φ l'opérateur linéaire de l'espace $\mathcal{V}$. Représentons les vecteurs $\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n)$ sous forme de combinaisons linéaires des vecteurs de la base (1):

$$(2) \quad \begin{aligned} \varphi(\mathbf{e}_1) &= \alpha_{11}\mathbf{e}_1 + \ldots + \alpha_{n1}\mathbf{e}_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ \varphi(\mathbf{e}_n) &= \alpha_{1n}\mathbf{e}_1 + \ldots + \alpha_{nn}\mathbf{e}_n. \end{aligned}$$

DEFINITION. La matrice $M(\varphi)$

$$M(\varphi) = \begin{bmatrix} \alpha_{11} \ldots \alpha_{1n} \\ \ldots\ldots \\ \alpha_{n1} \ldots \alpha_{nn} \end{bmatrix}$$

dont la k-ième colonne est la colonne de coordonnées du vecteur $\varphi(\mathbf{e}_k)$ relativement à la base (1), est appelée *matrice de l'opérateur linéaire* φ *relativement à la base* (1).

Rappelons que $F^{n\times n}$ désigne l'ensemble de toutes les matrices $n \times n$ sur le corps $\mathcal{F}$.

THEOREME 2.1. *Soit $\mathcal{V}$ un espace vectoriel sur le corps $\mathcal{F}$ avec une base* (1) *fixée. L'application Φ associant à chaque opérateur linéaire φ de l'espace $\mathcal{V}$ sa matrice $M(\varphi)$ relativement à la base* (1), *est une application bijective de l'ensemble* Hom $(\mathcal{V}, \mathcal{V})$ *sur l'ensemble* $F^{n\times n}$.

Démonstration. Φ est apparemment une application sur l'ensemble $F^{n\times n}$. Démontrons que l'application Φ est injective, c'est-à-dire que pour tous φ et ψ de l'égalité $M(\varphi) = M(\psi)$ s'ensuit l'égalité $\varphi = \psi$. De $M(\varphi) = M(\psi)$ se dégage l'égalité

$$M(\varphi(\mathbf{e}_k)) = M(\psi(\mathbf{e}_k)) \quad \text{pour} \quad k = 1, \ldots, n,$$

d'où

$$\varphi(\mathbf{e}_k) = \psi(\mathbf{e}_k) \quad \text{pour} \quad k = 1, \ldots, n.$$

Selon le corollaire 1.2, il s'ensuit l'égalité $\varphi = \psi$. □

Soit λ un scalaire, $\lambda \in F$. Notons ω'_λ l'opération singulaire (unaire) dans l'ensemble Hom $(\mathcal{U}, \mathcal{V})$ associant à chaque application linéaire $\varphi \in$ Hom $(\mathcal{U}, \mathcal{V})$ l'application linéaire $\lambda\varphi$:

$$\omega'_\lambda(\varphi) = \lambda\varphi.$$

Cette opération sera appelée *opération de multiplication par le scalaire* λ.

THEOREME 2.2. *Soient* $\mathcal{U}$, $\mathcal{V}$ *des espaces vectoriels sur le corps* $\mathcal{F}$. *L'algèbre*

$$\langle \mathrm{Hom}\,(\mathcal{U},\,\mathcal{V}),\ +,\ -,\ \{\omega'_\lambda \mid \lambda \in F\}\rangle$$

est un espace vectoriel sur le corps $\mathcal{F}$.

Démonstration. Selon le corollaire 1.2, l'ensemble Hom $(\mathcal{U}, \mathcal{V})$ est fermé par rapport à l'addition et aux opérations singulaires (unaires) ω'_λ de multiplication par des scalaires du corps $\mathcal{F}$.

Notons que « — » désigne une opération singulaire (unaire) dans l'ensemble Hom $(\mathcal{U}, \mathcal{V})$ associant à l'opérateur $\varphi \in$ Hom $(\mathcal{U}, \mathcal{V})$ l'opérateur $-\varphi = (-1)\,\varphi$, et $\bar{0}$ l'application zéro de $\mathcal{U}$ dans $\mathcal{V}$. L'algèbre $\langle$Hom $(\mathcal{U}, \mathcal{V})$, $+$, $-\rangle$ est un groupe abélien. En effet, on vérifie sans peine que pour tous φ, ψ, $\chi \in$ Hom $(\mathcal{U}, \mathcal{V})$ on a les égalités

$$\varphi + \psi = \psi + \varphi, \qquad \varphi + \bar{0} = \varphi,$$
$$\varphi + (\psi + \chi) = (\varphi + \psi) + \chi, \qquad \varphi + (-\varphi) = \bar{0}.$$

En outre, on vérifie aisément que pour tous λ, $\mu \in F$, on a

$$\lambda\,(\varphi + \psi) = \lambda\varphi + \lambda\psi, \qquad (\lambda\mu)\,\varphi = \lambda\,(\mu\varphi),$$
$$(\lambda + \mu)\,\varphi = \lambda\varphi + \mu\varphi, \qquad 1\cdot\varphi = \varphi.$$

Ainsi, tous les axiomes de l'espace vectoriel se vérifient. □

L'espace vectoriel

$$\langle \mathrm{Hom}\,(\mathcal{U},\,\mathcal{V}),\ +,\ -,\ \{\omega'_\lambda \mid \lambda \in F\}\rangle$$

sera appelé *espace vectoriel des applications linéaires* $\mathcal{U}$ *dans* $\mathcal{V}$ et on le notera $\mathcal{H}om\,(\mathcal{U}, \mathcal{V})$.

Connexion entre les colonnes de coordonnées des vecteurs x et $\boldsymbol{\varphi}$**(x).** Soient

(1) $\mathbf{e}_1, \ldots, \mathbf{e}_n$

la base fixée de l'espace vectoriel $\mathcal{V}$ et φ l'opérateur linéaire de cet espace. Soient, ensuite,

$$\mathbf{x} = \xi_1\mathbf{e}_1 + \ldots + \xi_n\mathbf{e}_n \text{ et } \varphi\,(\mathbf{x}) = \eta_1\mathbf{e}_1 + \ldots + \eta_n\mathbf{e}_n.$$

Notons $M\,(\mathbf{x})$ et $M\,(\varphi\,(\mathbf{x}))$ les colonnes de coordonnées respectivement des vecteurs $\mathbf{x}$ et $\varphi\,(\mathbf{x})$ relativement à la base fixée (1):

$$M\,(\mathbf{x}) = \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix}, \qquad M\,(\varphi\,(\mathbf{x})) = \begin{bmatrix} \eta_1 \\ \vdots \\ \eta_n \end{bmatrix}.$$

Cherchons la connexion entre ces colonnes de coordonnées.

THÉORÈME 2.3. *Soient* φ *l'opérateur linéaire de l'espace vectoriel* $\mathcal{V}$ *et* $M(\varphi)$ *la matrice de l'opérateur* φ *relativement à la base* (1). *Alors pour tout vecteur* $\mathbf{x} \in V$ *est satisfaite l'égalité*

$$M(\varphi(\mathbf{x})) = M(\varphi) M(\mathbf{x}).$$

Démonstration. Soit

$$M(\varphi) = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \cdot & \cdot & \cdot \\ \alpha_{n1} & \dots & \alpha_{nn} \end{bmatrix},$$

les égalités (2) sont alors vérifiées. Si $\mathbf{x} = \xi_1\mathbf{e}_1 + \dots + \xi_n\mathbf{e}_n \in V$, alors

$$\varphi(\mathbf{x}) = \xi_1\varphi(\mathbf{e}_1) + \dots + \xi_n\varphi(\mathbf{e}_n).$$

En substituant sur la base de (2) dans cette égalité les vecteurs $\varphi(\mathbf{e}_1), \dots, \varphi(\mathbf{e}_n)$, il vient

$$\varphi(\mathbf{x}) = \xi_1(\alpha_{11}\mathbf{e}_1 + \dots + \alpha_{n1}\mathbf{e}_n) + \dots + \xi_n(\alpha_{1n}\mathbf{e}_1 + \dots + \alpha_{nn}\mathbf{e}_n),$$

d'où

$$\varphi(\mathbf{x}) = (\alpha_{11}\xi_1 + \dots + \alpha_{1n}\xi_n)\mathbf{e}_1 + \dots + (\alpha_{n1}\xi_1 + \dots + \alpha_{nn}\xi_n)\mathbf{e}_n.$$

Donc,

$$M(\varphi(\mathbf{x})) = \begin{bmatrix} \alpha_{11}\xi_1 + \dots + \alpha_{1n}\xi_n \\ \dots\dots\dots\dots \\ \alpha_{n1}\xi_1 + \dots + \alpha_{nn}\xi_n \end{bmatrix} = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \cdot & \cdot & \cdot \\ \alpha_{n1} & \dots & \alpha_{nn} \end{bmatrix} \cdot \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix},$$

c'est-à-dire $M(\varphi(\mathbf{x})) = M(\varphi) M(\mathbf{x})$. □

THÉORÈME 2.4. *Soient* φ *l'opérateur linéaire de l'espace vectoriel* $\mathcal{V}$ *et* $M(\varphi)$ *la matrice de l'opérateur* φ *relativement à la base fixée* (1). *Si pour tout vecteur* $\mathbf{x} \in V$ *on a*

(3) $\quad M(\varphi(\mathbf{x})) = BM(\mathbf{x}),$

alors $B = M(\varphi)$.

Démonstration. Selon la définition de la matrice $M(\varphi)$,

(4) $\quad M(\varphi) = (M(\varphi(\mathbf{e}_1)), M(\varphi(\mathbf{e}_2)), \dots, M(\varphi(\mathbf{e}_n))).$

En portant successivement dans (3) au lieu de $\mathbf{x}$ les vecteurs de base $\mathbf{e}_1, \ldots, \mathbf{e}_n$, il vient

$$M(\varphi(\mathbf{e}_1)) = BM(\mathbf{e}_1) = B\begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix} = B^1;$$

(5) $$M(\varphi(\mathbf{e}_2)) = BM(\mathbf{e}_2) = B\begin{bmatrix}0\\1\\\vdots\\0\end{bmatrix} = B^2;$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$M(\varphi(\mathbf{e}_n)) = BM(\mathbf{e}_n) = B\begin{bmatrix}0\\0\\\vdots\\1\end{bmatrix} = B^n.$$

Sur la base de (4) et (5) on conclut que les colonnes correspondantes des matrices $M(\varphi)$ et B coïncident. Par conséquent, $M(\varphi) = B$. □

PROPOSITION 2.5. *Soient φ et ψ les opérateurs linéaires de l'espace vectoriel $\mathcal{V}$ à base fixée $\mathbf{e}_1, \ldots, \mathbf{e}_n$ et $\lambda \in F$; alors*

(1) $M(\varphi + \psi) = M(\varphi) + M(\psi)$;

(2) $M(\lambda\varphi) = \lambda M(\varphi)$.

Démonstration. Soient $\mathbf{x} \in V$ et

(3)
$$\varphi(\mathbf{x}) = \xi_1\mathbf{e}_1 + \ldots + \xi_n\mathbf{e}_n;$$
$$\psi(\mathbf{x}) = \eta_1\mathbf{e}_1 + \ldots + \eta_n\mathbf{e}_n,$$

alors

$$(\varphi + \psi)(\mathbf{x}) = (\xi_1 + \eta_1)\mathbf{e}_1 + \ldots + (\xi_n + \eta_n)\mathbf{e}_n.$$

Donc,

$$M((\varphi + \psi)(\mathbf{x})) = \begin{bmatrix}\xi_1 & +\eta_1\\ \cdots & \cdots\\ \xi_n & \eta_n\end{bmatrix} = \begin{bmatrix}\xi_1\\\vdots\\\xi_n\end{bmatrix} + \begin{bmatrix}\eta_1\\\vdots\\\eta_n\end{bmatrix} =$$
$$= M(\varphi(\mathbf{x})) + M(\psi(\mathbf{x}))$$

et, selon le théorème 2.3,

(4) $M((\varphi + \psi)(\mathbf{x})) = (M(\varphi) + M(\psi))M(\mathbf{x})$.

L'égalité (4) est vraie pour tout $x \in V$. Selon le théorème 2.4, de (4) s'ensuit l'égalité (1).

En vertu de (3), $(\lambda\varphi)(\mathbf{x}) = \lambda\xi_1\mathbf{e}_1 + \ldots + \lambda\xi_n\mathbf{e}_n$; donc,

$$M((\lambda\varphi)(\mathbf{x})) = \lambda M(\varphi(\mathbf{x}))$$

et, selon le théorème 2.3, pour tout $\mathbf{x}$, on a

(5) $$M((\lambda\varphi)(\mathbf{x})) = (\lambda M(\varphi)) M(\mathbf{x}).$$

Selon le théorème 2.4, de (5) s'ensuit (2). □

Rang d'un opérateur linéaire. Etablissons la connexion entre le rang d'un opérateur linéaire et le rang de sa matrice.

THEOREME 2.6. *Le rang d'un opérateur linéaire d'un espace vectoriel de dimension finie* $\neq \{0\}$ *est égal au rang de la matrice de cet opérateur.*

Démonstration. Soit $\mathbf{e}_1, \ldots, \mathbf{e}_n$ la base fixée de l'espace vectoriel $\mathscr{V}$. Soient $M(\varphi(\mathbf{e}_1)), \ldots, M(\varphi(\mathbf{e}_n))$ les colonnes de coordonnées des vecteurs $\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n)$ relativement à la base fixée. Ce sont des colonnes de la matrice $M(\varphi)$ de l'opérateur φ relativement à la base fixée, c'est-à-dire

$$M(\varphi) = (M(\varphi(\mathbf{e}_1)), \ldots, M(\varphi(\mathbf{e}_n))).$$

Donc,

(1) $$\text{rang } M(\varphi) = \text{rang } (M(\varphi(\mathbf{e}_1)), \ldots, M(\varphi(\mathbf{e}_n))).$$

En vertu du corollaire 7.3, le rang du système des vecteurs $\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n)$ est égal au rang du système de colonnes de ces vecteurs. De là et à partir de (1) il s'ensuit que

(2) $$\text{rang } M(\varphi) = \text{rang } (\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n)).$$

Soient $\mathbf{x}$ un vecteur arbitraire de l'espace $\mathscr{V}$ et $\mathbf{x} = \xi_1\mathbf{e}_1 + \ldots + \xi_n\mathbf{e}_n$. En vertu de la linéarité de l'opérateur φ l'égalité $\varphi(\mathbf{x}) = \xi_1\varphi(\mathbf{e}_1) + \ldots + \xi_n\varphi(\mathbf{e}_n)$ se vérifie. Aussi a-t-on

$$\text{Im}(\varphi) = L(\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n)),$$

c'est-à-dire que l'image de l'opérateur φ est engendrée par les vecteurs $\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n)$. Selon le corollaire 7.3, il s'ensuit que

(3) $$\text{rang } \varphi = \text{rang } (\varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n)).$$

Sur la base de (2) et (3) on conclut que le rang φ est égal au rang de la matrice $M(\varphi)$. □

Connexion entre les colonnes de coordonnées d'un vecteur relativement à de différentes bases. Soit $\mathscr{V}$ un espace vectoriel de dimension $n \neq \{0\}$ sur le corps $\mathscr{F}$. Soient données deux bases de cet espace : $\mathbf{e}_1, \ldots, \mathbf{e}_n$, la première base et $\mathbf{e}'_1, \ldots, \mathbf{e}'_n$, la deuxième. Les vecteurs de la deuxième base seront représentés sous forme des combi-

naisons linéaires de la première base:

$$
\begin{array}{ll}
 & \mathbf{e}_1' = t_{11}\mathbf{e}_1 + \ldots + t_{n1}\mathbf{e}_n \\
(1) & \ldots\ldots\ldots\ldots\ldots\ldots \qquad (t_{ik} \in F). \\
 & \mathbf{e}_n' = t_{1n}\mathbf{e}_1 + \ldots + t_{nn}\mathbf{e}_n
\end{array}
$$

On appelle *matrice de passage de la première base à la deuxième* la matrice T,

$$T = \begin{bmatrix} t_{11} & t_{12} & \ldots & t_{1n} \\ t_{21} & t_{22} & \ldots & t_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ t_{n1} & t_{n2} & \ldots & t_{nn} \end{bmatrix},$$

dont la k-ième colonne est la colonne de coordonnées du vecteur $\mathbf{e}_k'$ relativement à la première base.

PROPOSITION 2.7. *La matrice T est inversible.*

Démonstration. Il s'ensuit de l'indépendance linéaire des vecteurs $\mathbf{e}_1', \ldots, \mathbf{e}_n'$ l'indépendance linéaire des colonnes de coordonnées de ces vecteurs, autrement dit, l'indépendance linéaire des colonnes de la matrice T (voir corollaire 7.4). Il s'ensuit, selon le théorème 5.1, que la matrice T est inversible. □

Notons $M(\mathbf{x})$ la colonne de coordonnées du vecteur $\mathbf{x} \in V$ relativement à la première base et $M'(\mathbf{x})$ relativement à la deuxième base. Cherchons la relation entre $M(\mathbf{x})$ et $M'(\mathbf{x})$.

THÉORÈME 2.8. *Soient $M(\mathbf{x})$ et $M'(\mathbf{x})$ les colonnes de coordonnées du vecteur $\mathbf{x}$ respectivement relativement à la première et à la deuxième bases et T la matrice de passage de la première base de l'espace à la deuxième. On a alors les égalités*

(2) $\quad M(\mathbf{x}) = TM'(\mathbf{x});$

(3) $\quad M'(\mathbf{x}) = T^{-1}M(\mathbf{x}).$

Démonstration. Soient $\mathbf{x} \in V$ et

(4) $\quad \mathbf{x} = \xi_1\mathbf{e}_1 + \ldots + \xi_n\mathbf{e}_n;$

(5) $\quad \mathbf{x} = \xi_1'\mathbf{e}_1' + \ldots + \xi_n'\mathbf{e}_n';$

par conséquent,

$$M(\mathbf{x}) = \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix}, \qquad M'(\mathbf{x}) = \begin{bmatrix} \xi_1' \\ \vdots \\ \xi_n' \end{bmatrix}.$$

Portons dans (5) les expressions de $\mathbf{e}_1', \ldots, \mathbf{e}_n'$ des égalités (1), il vient

$$\mathbf{x} = \xi_1'(t_{11}\mathbf{e}_1 + \ldots + t_{n1}\mathbf{e}_n) + \ldots + \xi_n'(t_{1n}\mathbf{e}_1 + \ldots \\ \ldots + t_{nn}\mathbf{e}_n),$$

d'où

(6) $\mathbf{x} = (t_{11}\xi_1' + \ldots + t_{1n}\xi_n')\,\mathbf{e}_1 + \ldots$
$\ldots + (t_{n1}\xi_1' + \ldots + t_{nn}\xi_n')\,\mathbf{e}_n.$

A partir de (4) et (6) on déduit les égalités

$$\xi_1 = t_{11}\xi_1' + \ldots + t_{1n}\xi_n';$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\xi_n = t_{n1}\xi_1' + \ldots + t_{nn}\xi_n'.$$

De là on obtient l'égalité

$$\begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix} = T \begin{bmatrix} \xi_1' \\ \vdots \\ \xi_n' \end{bmatrix},$$

c'est à-dire que $M(\mathbf{x}) = TM'(\mathbf{x})$. Multiplions à gauche les deux membres de cette égalité par T^{-1} et l'on obtient (3). □

COROLLAIRE 2.9. *Si* ${}^tM(\mathbf{x})$ *et* ${}^tM'(\mathbf{x})$ *sont des lignes de coordonnées du vecteur* $\mathbf{x}$ *respectivement par rapport à la priemère et à la deuxième bases, on obtient alors*

$${}^tM(\mathbf{x}) = {}^tM'(\mathbf{x})\,{}^tT, \qquad {}^tM'(\mathbf{x}) = {}^tM(\mathbf{x})\,{}^t(T^{-1}).$$

Connexion entre les matrices d'un opérateur linéaire relativement à de différentes bases. Soient $\mathscr{V}$ un espace vectoriel de dimension finie $\neq \{0\}$, $\mathbf{e}_1, \ldots, \mathbf{e}_n$ la première base de l'espace $\mathscr{V}$, $\mathbf{e}_1', \ldots, \mathbf{e}_n'$ la deuxième base de l'espace $\mathscr{V}$ et T la matrice de passage de la première à la deuxième base.

THÉORÈME 2.10. *Soient* φ *l'opérateur linéaire de l'espace vectoriel* $\mathscr{V}$, $M(\varphi)$ *et* $M'(\varphi)$ *les matrices de cet opérateur respectivement par rapport à la première et à la deuxième bases et* T *la matrice de passage de la première à la deuxième base, on a alors* $M'(\varphi) = T^{-1}M(\varphi)\,T$.

D é m o n s t r a t i o n. Selon le théorème 2.8 pour tout $\mathbf{x} \in V$, on a

(2) $M(\mathbf{x}) = TM'(\mathbf{x});$

(3) $M'(\mathbf{x}) = T^{-1}M(\mathbf{x}),$

où $M(\mathbf{x})$ et $M'(\mathbf{x})$ sont des colonnes de coordonnées du vecteur $\mathbf{x}$ respectivement par rapport à la première et à la deuxième bases. En substituant dans (3) $\varphi(\mathbf{x})$ à $\mathbf{x}$, il vient

$$M'(\varphi(\mathbf{x})) = T^{-1}M(\varphi(\mathbf{x})).$$

Selon le théorème 2.3, $M(\varphi(\mathbf{x})) = M(\varphi)\,M(\mathbf{x})$, donc,

$$M'(\varphi(\mathbf{x})) = T^{-1}M(\varphi)\,M(\mathbf{x}).$$

En vertu de (2), il vient

$$M'(\varphi(\mathbf{x})) = [T^{-1}M(\varphi)\,T]\,M'(\mathbf{x}).$$

Etant donné que cette égalité se vérifie pour tout $\mathbf{x}$ de V, on a, en vertu du théorème 2.4, $M'(\varphi) = T^{-1}M(\varphi)\,T$. □

DEFINITION. Les matrices A et B de l'ensemble $F^{n\times n}$ sont dites *semblables sur le corps* $\mathcal{F}$ s'il existe une matrice inversible $T \in F^{n\times n}$ telle que $A = T^{-1}BT$.

Du théorème 2.10 découle le corollaire suivant.

COROLLAIRE 2.11. *Si φ est un opérateur linéaire de l'espace vectoriel $\mathcal{V}$ de dimension finie non réduit à $\{0\}$, alors les matrices de cet opérateur rapportées à deux bases quelconques de l'espace sont semblables.*

PROPOSITION 2.12. *La relation de similitude des matrices sur l'ensemble $F^{n\times n}$ est une ralation d'équivalence.*

Démonstration. La relation de similitude est réflexive, car $A = E^{-1}AE$, où E est une matrice unité. La relation de similitude est symétrique, car de l'égalité $A = T^{-1}BT$ s'ensuit $B = (T^{-1})^{-1}AT^{-1}$. La relation de similitude est transitive, car de $A = T^{-1}BT$ et $B = T_1^{-1}CT_1$ s'ensuit

$$A = (T_1T)^{-1}C\,(T_1T).$$

La relation de similitude des matrices sur le corps $\mathcal{F}$ définit la partition de l'ensemble $F^{n\times n}$ en classes d'équivalence appelées *classes de matrices semblables.* A chaque opérateur linéaire de l'espace vectoriel $\mathcal{V}$ est associée une classe unique de matrices semblables.

Exercices

1. Comment variera la matrice d'un opérateur linéaire si l'on permute dans la base $\mathbf{e}_1, \ldots, \mathbf{e}_n$ deux quelconques des vecteurs, par exemple, $\mathbf{e}_1$ et $\mathbf{e}_2$?

2. Démontrer que le rang de l'opérateur linéaire d'un espace vectoriel de dimension finie est égal au rang de la matrice de cet opérateur.

3. Montrer que tout opérateur linéaire de rang r d'un espace vectoriel de dimension finie peut être représenté sous forme d'une somme de r opérateurs linéaires de rang 1.

4. Soit $\mathcal{V}$ un espace vectoriel de toutes les matrices carrées d'ordre deux sur le corps $\mathcal{F}$. Montrer que la transformation φ consistant dans la multiplication des matrices de $\mathcal{V}$ à gauche par la matrice $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ est un opérateur linéaire. Chercher la matrice de l'opérateur φ dans la base

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

5. Démontrer que l'opérateur linéaire φ de l'espace vectoriel de dimension finie $\mathcal{V}$, permutable avec chaque opérateur linéaire de l'espace $\mathcal{V}$, est un scalaire, c'est-à-dire qu'il existe un scalaire λ tel que $\varphi(\mathbf{x}) = \lambda\mathbf{x}$ pour tout vecteur $\mathbf{x}$ de $\mathcal{V}$.

6. Soient φ un opérateur linéaire quelconque, ψ un opérateur linéaire inversible de l'espace vectoriel de dimension finie. Démontrer que rang $(\varphi\psi) =$ rang $(\psi\varphi) =$ rang φ.

7. Soient φ, ψ des opérateurs linéaires quelconques d'un espace vectoriel de dimension finie. Démontrer que:

(a) $\operatorname{rang}(\varphi + \psi) \leqslant \operatorname{rang} \varphi + \operatorname{rang} \psi$;

(b) $\operatorname{rang}(\varphi\psi) \leqslant \operatorname{rang} \varphi$, $\operatorname{rang}(\varphi\psi) \leqslant \operatorname{rang} \psi$;

(c) $\operatorname{déf} \varphi \leqslant \operatorname{déf}(\varphi\psi) \leqslant \operatorname{déf} \varphi + \operatorname{déf} \psi$.

8. Donner un exemple d'opérateurs linéaires φ, ψ d'un espace vectoriel bidimensionnel pour lesquels $\operatorname{rang}(\varphi, \psi) \neq \operatorname{rang}(\psi\varphi)$.

9. Démontrer que pour tous opérateurs linéaires φ, ψ d'un espace vectoriel de dimension n est satisfaite l'inégalité

$$\operatorname{rang}(\varphi\psi) \geqslant \operatorname{rang} \varphi + \operatorname{rang} \psi - n.$$

10. Soit φ un opérateur linéaire de l'espace vectoriel $\mathcal{V}$. Le sous-espace $\mathcal{L}$ de l'espace $\mathcal{V}$ est dit *invariant relativement à* φ si $\varphi(L) \subset L$. Supposons que l'opérateur φ possède relativement à la base $\mathbf{e}_1, \ldots, \mathbf{e}_n$ une matrice diagonale à éléments diagonaux différents. Chercher tous les sous-espaces de l'espace $\mathcal{V}$ invariants relativement à φ et montrer que leur nombre vaut 2^n.

§ 3. Algèbres linéaires

Algèbre linéaire. Soit $\mathcal{F}$ un corps des scalaires.

DÉFINITION. L'algèbre $\langle V, +, \{\omega_\lambda \mid \lambda \in F\}, \cdot\rangle$ est appelée *algèbre linéaire* si les opérations binaires $+$, $\cdot$ et les opérations singulaires ω_λ satisfont aux exigences suivantes:

1) l'algèbre $\langle V, +, \{\omega_\lambda \mid \lambda \in F\}\rangle$ est un espace vectoriel sur le corps $\mathcal{F}$;

2) les conditions de bilinéarité sont remplies, c'est-à-dire

$$(\mathbf{a} + \mathbf{b})\,\mathbf{c} = \mathbf{ac} + \mathbf{bc}, \qquad \mathbf{c}\,(\mathbf{a} + \mathbf{b}) = \mathbf{ca} + \mathbf{cb},$$
$$\omega_\lambda(\mathbf{ab}) = (\omega_\lambda \mathbf{a})\,\mathbf{b} = \mathbf{a}\,(\omega_\lambda \mathbf{b})$$

pour tous $\mathbf{a}, \mathbf{b}, \mathbf{c} \in V$ et tout $\lambda \in F$.

On appelle *rang de l'algèbre linéaire* la dimension de l'espace vectoriel $\langle V, +, \{\omega_\lambda \mid \lambda \in F\}\rangle$.

E x e m p l e s. 1. Soit $\mathbf{C}$ l'ensemble de tous les nombres complexes. L'algèbre

$$\langle \mathbf{C}, +, \{\omega_\lambda \mid \lambda \in \mathbf{R}\}, \cdot\rangle$$

est une algèbre linéaire sur le corps $\mathcal{R}$ des nombres réels. Son rang vaut deux.

2. Soit $F^{n\times n}$ un ensemble de toutes les matrices $n \times n$ sur un corps. L'algèbre

$$\langle F^{n\times n}, +, \{\omega_\lambda \mid \lambda \in F\}, \cdot\rangle,$$

où ω_λ est une opération singulaire (unaire) de multiplication par le scalaire λ, constitue une algèbre linéaire sur le corps $\mathcal{F}$ de rang n^2. On l appelle *algèbre matricielle complète sur le corps* $\mathcal{F}$. Son rang vaut n^2.

3. L'algèbre des quaternions sur le corps $\mathcal{R}$ étant fixée, soient $\mathcal{V}$ un espace vectoriel de dimension quatre sur le corps $\mathcal{R}$ et $\mathbf{e}$, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$

sa base. Définissons la multiplication des vecteurs de base par les égalités suivantes:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{e}, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \ \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j};$$

$\mathbf{ae} = \mathbf{ea}$ pour tout vecteur $\mathbf{a} \in \{\mathbf{e}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$.

Le produit de deux quaternions quelconques est défini par l'égalité

$$(\alpha\mathbf{e} + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k})(\alpha_1\mathbf{e} + \beta_1\mathbf{i} + \gamma_1\mathbf{j} + \delta_1\mathbf{k}) = \\ = (\alpha\alpha_1 - \beta\beta_1 - \gamma\gamma_1 - \delta\delta_1)\mathbf{e} + \\ + (\alpha\beta_1 + \beta\alpha_1 + \gamma\delta_1 - \delta\gamma_1)\mathbf{i} + \\ + (\alpha\gamma_1 + \alpha_1\gamma + \delta\beta_1 - \beta\delta_1)\mathbf{j} + \\ + (\alpha\delta_1 + \alpha_1\delta + \beta\gamma_1 - \gamma\beta_1)\mathbf{k}.$$

Les quaternions $\mathbf{q} = \alpha\mathbf{e} + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}$ et $\overline{\mathbf{q}} = \alpha\mathbf{e} - \beta\mathbf{i} - \gamma\mathbf{j} - \delta\mathbf{k}$ sont dits *conjugués*. Le nombre réel

$$\mathcal{N}(\mathbf{q}) = \mathbf{q}\cdot\overline{\mathbf{q}} = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$$

est appelé *norme du quaternion.*

Une vérification directe montre que les conditions de bilinéarité sont satisfaites. L'algèbre

$$\langle V, +, \{\omega_\lambda \mid \lambda \in \mathbf{R}\}, \cdot\rangle$$

est donc linéaire. On l'appelle *algèbre des quaternions* sur le corps des nombres réels. On vérifie aisément que l'algèbre $\langle V, +, -, \cdot, \mathbf{e}\rangle$ est un anneau non commutatif, dans lequel pour tous $\mathbf{a}, \mathbf{b} \in V$ avec $\mathbf{a} \neq \mathbf{0}$ l'équation $\mathbf{ax} = \mathbf{b}$ est résoluble.

Algèbre d'opérateurs linéaires d'un espace vectoriel. Soient $\mathscr{V}$ un espace vectoriel sur le corps $\mathscr{F}$ et φ, ψ des opérateurs linéaires de cet espace. Le produit $\varphi\psi$ est défini comme composition de φ et ψ, c'est-à-dire comme application de l'espace $\mathscr{V}$ dans lui-même associant à l'élément $\mathbf{x}$ de V l'élément $\varphi(\psi(\mathbf{x}))$:

$$(\varphi\psi)(\mathbf{x}) = \varphi(\psi(\mathbf{x})).$$

PROPOSITION 3.1. *Un produit de deux quelconques opérateurs linéaires de l'espace vectoriel $\mathscr{V}$ est un opérateur linéaire de cet espace.*

Démonstration. Soient φ et ψ des opérateurs linéaires de l'espace $\mathscr{V}$. Le produit $\varphi\psi$ satisfait aux conditions de linéarité. En effet, si $\mathbf{x}, \mathbf{y} \in V$ et $\lambda \in F$, alors

$$(\varphi\psi)(\mathbf{x} + \mathbf{y}) = \varphi(\psi(\mathbf{x} + \mathbf{y})) = \varphi(\psi(\mathbf{x}) + \psi(\mathbf{y})) = \\ = \varphi(\psi(\mathbf{x})) + \varphi(\psi(\mathbf{y})) = (\varphi\psi)(\mathbf{x}) + (\varphi\psi)(\mathbf{y});$$

$$(\varphi\psi)(\lambda\mathbf{x}) = \varphi(\psi(\lambda\mathbf{x})) = \varphi(\lambda\psi(\mathbf{x})) = \lambda(\varphi(\psi(\mathbf{x}))) = \\ = \lambda((\varphi\psi)(\mathbf{x})).$$

Ainsi, le produit $\varphi\psi$ est un opérateur linéaire de l'espace $\mathscr{V}$. □

Soit $\mathscr{V}$ un espace vectoriel sur le corps $\mathscr{F}$. En vertu du corollaire 1.6, $\mathscr{H}om\,(\mathscr{V}, \mathscr{V})$ est un espace vectoriel sur le corps $\mathscr{F}$:

$$\mathscr{H}om\,(\mathscr{V}, \mathscr{V}) = \langle \mathrm{Hom}\,(\mathscr{V}, \mathscr{V}),\ +,\ \{\omega'_\lambda \mid \lambda \in F\}\rangle,$$

où ω'_λ est une opération singulaire (unaire) de multiplication d'opérateurs linéaires de l'espace $\mathscr{V}$ par le scalaire λ. Considérons l'algèbre

$$\langle \mathrm{Hom}\,(\mathscr{V}, \mathscr{V}),\ +,\ \{\omega'_\lambda \mid \lambda \in F\},\ \cdot\rangle,$$

où l'opération binaire « · » est une opération de multiplication d'opérateurs linéaires de l'espace $\mathscr{V}$; cette algèbre s'appelle *algèbre d'opérateurs linéaires de l'espace* $\mathscr{V}$ et est notée *End* $\mathscr{V}$.

THÉORÈME 3.2. *Soit $\mathscr{V}$ un espace vectoriel sur le corps $\mathscr{F}$. L'algèbre End $\mathscr{V}$ est une algèbre linéaire sur le corps $\mathscr{F}$.*

D é m o n s t r a t i o n. Selon le théorème 2.2, l'algèbre

$$\langle \mathrm{Hom}\,(\mathscr{V}, \mathscr{V}),\ +,\ \{\omega'_\lambda \mid \lambda \in F\}\rangle$$

est un espace vectoriel sur le corps $\mathscr{F}$. En outre, les conditions de bilinéarité sont satisfaites:

(1) $(\varphi + \psi)\,\chi = \varphi\chi + \psi\chi;$

(2) $\chi\,(\varphi + \psi) = \chi\varphi + \chi\psi;$

(3) $\lambda\,(\varphi\psi) = (\lambda\varphi)\,\psi = \varphi\,(\lambda\psi),$

où $\varphi, \psi, \chi \subset \mathrm{Hom}\,(\mathscr{V}, \mathscr{V})$ et $\lambda \in F$.

Démontrons l'égalité (1). Si $\mathbf{x} \in V$, alors

$$((\varphi + \psi)\,\chi)\,(\mathbf{x}) = (\varphi + \psi)\,(\chi\,(\mathbf{x})) = \varphi\,(\chi\,(\mathbf{x})) + \psi\,(\chi\,(\mathbf{x})) = \\ = (\varphi\chi)\,(\mathbf{x}) + (\psi\chi)\,(\mathbf{x}) = (\varphi\chi + \psi\chi)\,(\mathbf{x}),$$

c'est-à-dire qu'on aboutit à (1). De façon analogue, on démontre (2).

Démontrons la première des égalités de (3). Si $\mathbf{x} \in V$, alors

$$(\lambda\,(\varphi\psi))\,(\mathbf{x}) = \lambda\,((\varphi\psi)\,(\mathbf{x})) = \lambda\,(\varphi\,(\psi\,(\mathbf{x}))) = (\lambda\varphi)\,(\psi\,(\mathbf{x})) = \\ = ((\lambda\varphi)\,\psi)\,(\mathbf{x}),$$

c'est-à-dire $\lambda\,(\varphi\psi) = (\lambda\varphi)\,\psi$. De façon analogue, on démontre l'égalité $(\lambda\varphi)\,\psi = \varphi\,(\lambda\psi)$. □

Isomorphisme de l'algèbre d'opérateurs linéaires et de l'algèbre matricielle complète. Soient $\mathfrak{A}$ et $\mathfrak{A}'$ des algèbres linéaires sur le corps $\mathscr{F}$. L'application Φ de l'algèbre $\mathfrak{A}$ sur l'algèbre $\mathfrak{A}'$ est appelée *isomorphisme* si elle est injective et respecte les opérations principales de l'algèbre $\mathfrak{A}$, c'est-à-dire

$$\Phi\,(\mathbf{a} + \mathbf{b}) = \Phi\,(\mathbf{a}) + \Phi\,(\mathbf{b}), \quad \Phi\,(\lambda\mathbf{a}) = \lambda\Phi\,(\mathbf{a}), \\ \Phi\,(\mathbf{ab}) = \Phi\,(\mathbf{a})\,\Phi\,(\mathbf{b})$$

pour tous $\mathbf{a}, \mathbf{b} \in V$ et tout $\lambda \in F$. Les algèbres $\mathfrak{A}$ et $\mathfrak{A}'$ sont dites *isomorphes* s'il y a un isomorphisme de l'algèbre $\mathfrak{A}$ sur l'algèbre $\mathfrak{A}'$.

On vérifie sans peine que la relation d'isomorphisme d'une collection quelconque d'algèbres sur le corps $\mathcal{F}$ est une relation d'équivalence.

E x e m p l e. L'algèbre des nombres complexes

$$\langle \mathbf{C}, +, \{\omega_\lambda \mid \lambda \in \mathbf{R}\}, \cdot \rangle$$

est isomorphe à l'algèbre de toutes les matrices de la forme $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ sur $\mathcal{R}$:

$$\left\langle \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \middle| a, b \in \mathbf{R} \right\}, \quad +, \{\omega_\lambda \mid \lambda \in \mathbf{R}\}, \cdot \right\rangle.$$

Dans ce cas la correspondance

$$a + bi \mapsto \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

est établie par l'isomorphisme des algèbres linéaires considérées.

Notons $\mathfrak{M}(n, \mathcal{F})$ l'algèbre matricielle complète sur $\mathcal{F}$:

$$\mathfrak{M}(n, \mathcal{F}) = \langle F^{n \times n}, +, \{\omega_\lambda \mid \lambda \in F\}, \cdot \rangle.$$

THÉORÈME 3.3. *Soit $\mathcal{V}$ un espace vectoriel de dimension finie sur le corps $\mathcal{F}$ avec une base fixée* $\mathbf{e}_1, \ldots, \mathbf{e}_n$. *L'application associant à chaque opérateur linéaire φ de l'espace $\mathcal{V}$ sa matrice $M(\varphi)$ relativement à la base fixée constitue un isomorphisme de l'algèbre d'opérateurs linéaires End $\mathcal{V}$ sur l'algèbre matricielle complète $\mathfrak{M}(n, \mathcal{F})$.*

D é m o n s t r a t i o n. La correspondance de $\varphi \mapsto M(\varphi)$ est une application de l'ensemble *End* $\mathcal{V}$ = Hom $(\mathcal{V}, \mathcal{V})$ sur l'ensemble $\mathcal{F}^{n \times n}$ des matrices $n \times n$. En vertu du théorème 2.1, cette application est bijective. De plus, elle respecte toutes les opérations principales de l'algèbre *End* $\mathcal{V}$, c'est-à-dire

(1) $M(\varphi + \psi) = M(\varphi) + M(\psi)$,

(2) $M(\lambda\varphi) = \lambda M(\varphi)$,

(3) $M(\varphi\psi) = M(\varphi)\, M(\psi)$

pour tous $\varphi, \psi \in$ Hom $(\mathcal{V}, \mathcal{V})$ et tout $\lambda \in F$. Les égalités (1) et (2) ont été démontrées au paragraphe précédent.

Démontrons à présent l'égalité (3). Soit $\mathbf{x} \in V$. Alors $(\varphi\psi)(\mathbf{x}) = \varphi(\psi(\mathbf{x}))$ et, selon le théorème 2.3,

$$M((\varphi\psi)(\mathbf{x})) = M(\varphi(\psi(\mathbf{x}))) = M(\varphi)\,\mathrm{M}(\psi(\mathbf{x})) = [M(\varphi)\, M(\psi)]\, M(\mathbf{x}).$$

Ainsi, pour tout vecteur $\mathbf{x} \in V$, on a

$$M((\varphi\psi)(\mathbf{x})) = [M(\varphi) M\psi] M(\mathbf{x}).$$

Selon le théorème 2.4, il s'ensuit l'égalité (3).

Par conséquent, l'application considérée est un isomorphisme de l'algèbre $End\,\mathcal{V}$ sur l'algèbre $\mathfrak{M}(n, \mathcal{F})$.

Exercices

1. Démontrer que la multiplication des quaternions est associative.

2. Démontrer que dans l'algèbre des quaternions le système d'équations

$$\mathbf{i}x + \mathbf{j}y = \mathbf{e}, \qquad \mathbf{k}x - \mathbf{e}y = \mathbf{i}$$

admet une solution unique, tandis que le système

$$x\mathbf{i} + y\mathbf{j} = \mathbf{e}, \qquad x\mathbf{k} - \mathbf{e}y = \mathbf{i}$$

n'a pas de solutions.

3. Soient $\mathbf{a} = \alpha\mathbf{e} + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}$ un quaternion et $\mathbf{a}^* = \alpha\mathbf{e} - \beta\mathbf{i} - \gamma\mathbf{j} - \delta\mathbf{k}$. Montrer que pour tous quaternions $\mathbf{a}$, $\mathbf{b}$, on a

(a) $N(\mathbf{a}) = \mathbf{a}\mathbf{a}^* = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$;

(b) $N(\mathbf{ab}) = N(\mathbf{a})\, N(\mathbf{b})$;

(c) $(\mathbf{ab})^* = \mathbf{b}^*\mathbf{a}^*$.

4. Montrer qu'il existe un nombre infini de quaternions satisfaisant à l'équation $\mathbf{x}^2 + \mathbf{e} = 0$.

5. Soit $\mathbf{a} = \alpha\mathbf{e} + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}$ un quaternion quelconque. Vérifier que les quaternions $\mathbf{a}$ et $\mathbf{a}^*$ sont des racines de l'équation $\mathbf{x}^2 - 2\alpha\mathbf{x} + N(\mathbf{a})\,\mathbf{e} = 0$.

6. Montrer que si le quaternion $\mathbf{a}$ n'est pas un nombre réel il n'existe que deux quaternions satisfaisant à l'équation $\mathbf{x}^2 = \mathbf{a}$.

7. Démontrer que pour tous deux quaternions $\mathbf{a}$ et $\mathbf{b}$, on a

$$(\mathbf{a}\mathbf{a}^*)(\mathbf{b}\mathbf{b}^*) = (\mathbf{ab})(\mathbf{ab})^*.$$

En déduire que si chacun des nombres m, n est une somme des carrés de quatre entiers, alors le produit mn est également une somme des carrés de quatre entiers.

8. Démontrer qu'en algèbre des quaternions chacune des équations $\mathbf{ax} = \mathbf{b}$, $\mathbf{ya} = \mathbf{b}$ avec $\mathbf{a} \neq 0$ admet une solution unique.

9. Montrer que l'ensemble de tous les quaternions différents de zéro constitue un groupe par rapport à la multiplication.

10. Montrer que huit quaternions $\pm\mathbf{e}$, $\pm\mathbf{i}$, $\pm\mathbf{j}$, $\pm\mathbf{k}$ forment un groupe multiplicatif (il s'appelle *groupe quaternionique*).

11. Soit $\mathfrak{A}$ une algèbre de rang n sur le corps $\mathcal{F}$. Montrer qu'avec $k > n$ tous k éléments de l'algèbre $\mathfrak{A}$ sont linéairement dépendants sur le corps $\mathcal{F}$.

12. Soient respectivement 1, I, J, K des matrices complexes

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \quad \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix},$$

où $i = \sqrt{-1}$. Montrer que $I^2 = J^2 = K^2 = -1$, $IJ = -JI = K$, $JK = -KJ = I$, $KI = -IK = J$.

13. Démontrer que l'algèbre des matrices de la forme

$$\begin{bmatrix} \alpha+\beta i & \gamma+\delta i \\ -\gamma+\delta i & \alpha-\beta i \end{bmatrix}$$

avec α, β, γ, δ réels et $i = \sqrt{-1}$ est isomorphe à l'algèbre des quaternions sur le corps des nombres réels.

§ 4. Opérateurs inversibles

Opérateurs inversibles. Soient φ un opérateur linéaire de l'espace vectoriel $\mathscr{V}$ et ε un opérateur identique de cet espace. L'opérateur φ est dit *inversible* s'il existe un opérateur linéaire ψ de l'espace $\mathscr{V}$ tel que

(1) $\varphi\psi = \varepsilon, \quad \psi\varphi = \varepsilon.$

Il n'y a qu'un seul opérateur ψ répondant aux conditions (1). En effet, si l'opérateur ψ_1 satisfait aux conditions $\varphi\psi_1 = \varepsilon$, $\psi_1\varphi = \varepsilon$, alors

$$\psi_1 = \psi_1\varepsilon = \psi_1(\varphi\psi) = (\psi_1\varphi)\psi = \varepsilon\psi = \psi,$$

c'est-à-dire $\psi_1 = \psi$.

L'opérateur linéaire ψ satisfaisant aux conditions (1) s'appelle *opérateur inverse de l'opérateur* φ et est noté φ^{-1}.

THÉORÈME 4.1. *Soit φ un opérateur linéaire d'un espace vectoriel $\mathscr{V}$ de dimension finie $\neq \{0\}$. Les conditions suivantes sont alors équipotentes:*

(a) *l'opérateur φ est inversible;*
(b) *φ est une application injective de $\mathscr{V}$ sur $\mathscr{V}$;*
(c) Ker $\varphi = \{0\}$;
(d) déf $\varphi = 0$;
(e) rang $\varphi = \dim \mathscr{V}$;
(f) *la matrice de l'opérateur φ relativement à toute base de l'espace $\mathscr{V}$ est inversible.*

D é m o n s t r a t i o n. Soient φ un opérateur inversible et ψ l'opérateur inverse de φ. Démontrons que φ est injectif, c'est-à-dire que pour tous $\mathbf{a}, \mathbf{b} \in V$ il s'ensuit de $\varphi(\mathbf{a}) = \varphi(\mathbf{b})$ que $\mathbf{a} = \mathbf{b}$. En effet, si $\varphi(\mathbf{a}) = \varphi(\mathbf{b})$, alors

$$\psi(\varphi(\mathbf{a})) = \psi(\varphi(\mathbf{b})), \quad (\psi\varphi)(\mathbf{a}) = (\psi\varphi)(\mathbf{b}),$$
$$\varepsilon(\mathbf{a}) = \varepsilon(\mathbf{b}), \quad \mathbf{a} = \mathbf{b}.$$

De plus, φ est une application sur V, c'est-à-dire que pour tout $\mathbf{a} \in V$ on a une image anticipée. En effet,

$$\varphi(\psi(\mathbf{a})) = (\varphi\psi)\mathbf{a} = \varepsilon\mathbf{a} = \mathbf{a},$$

c'est-à-dire que $\psi(\mathbf{a})$ est l'image anticipée de $\mathbf{a}$ dans l'application φ.

Si φ est une injection, le vecteur nul $\mathbf{0}$ possède une image anticipée unique dans l'application φ, c'est-à-dire Ker $\varphi = \{\mathbf{0}\}$.

Si Ker $\varphi = \{\mathbf{0}\}$, la dimension du noyau de l'opérateur φ est nulle, c'est-à-dire déf $\varphi = 0$.

Si déf $\varphi = 0$, alors, selon le théorème 1.4, rang $\varphi = \dim \mathscr{V}$.

Supposons que rang $\varphi = \dim \mathscr{V} = n$. Soient $\mathbf{e}_1, \ldots, \mathbf{e}_n$ la base fixée de l'espace $\mathscr{V}$. Selon le théorème 2.6, le rang de la matrice

$M(\varphi)$ est égal à celui de l'opérateur φ et, par suite, vaut n. Ainsi, les lignes de la matrice $M(\varphi)$ sont linéairement indépendantes. Par conséquent, selon le théorème 5.1, la matrice $M(\varphi)$ est inversible.

Posons que la matrice $M(\varphi)$ est inversible et B est sa matrice inverse, c'est-à-dire

$$M(\varphi)\, B = E \text{ et } BM(\varphi) = E.$$

Selon le théorème 2.1, il existe un opérateur linéaire ψ de l'espace $\mathcal{V}$ tel que B soit la matrice de l'opérateur ψ relativement à la base fixée, c'est-à-dire $B = M(\varphi)$. En outre, $M(\varepsilon) = E$, par conséquent,

$$M(\varphi)\, M(\psi) = M(\varepsilon) \text{ et } M(\psi)\, M(\varphi) = M(\varepsilon).$$

En vertu du théorème 3.3, $M(\varphi)\, M(\psi) = M(\varphi\psi)$ et $M(\psi)\, M(\varphi) = M(\psi\varphi)$, aussi a-t-on

$$M(\varphi\psi) = M(\varepsilon), \quad M(\psi\varphi) = M(\varepsilon).$$

Selon le théorème 2.1, il s'ensuit les égalités $\varphi\psi = \varepsilon$ et $\psi\varphi = \varepsilon$, c'est-à-dire que l'opérateur φ est inversible. □

Groupe linéaire complet. Selon le théorème 5.1, l'ensemble de toutes les matrices inversibles $n \times n$ sur le corps $\mathcal{F}$ est un groupe par rapport aux opérations de multiplication et d'inversion.

DÉFINITION. Un groupe multiplicatif de toutes les matrices inversibles $n \times n$ sur le corps $\mathcal{F}$ est dit *groupe linéaire complet de degré n sur le corps* $\mathcal{F}$ et est noté $GL(n, \mathcal{F})$.

On voit aisément que tout opérateur inversible de l'espace vectoriel $\mathcal{V}$ est un automorphisme de cet espace. Inversement, tout automorphisme de l'espace $\mathcal{V}$ est un opérateur inversible. L'ensemble de tous les opérateurs inversibles de l'espace vectoriel $\mathcal{V}$ est noté Aut $\mathcal{V}$.

Considérons l'algèbre $\langle \text{Aut}\, \mathcal{V}, \cdot, {}^{-1} \rangle$, où $\cdot$ est une opération binaire de multiplication d'opérateurs linéaires de l'espace $\mathcal{V}$ et ${}^{-1}$ une opération de formation de l'opérateur inverse de l'opérateur donné ; cette algèbre sera désignée par le symbole $\mathcal{A}ut\, \mathcal{V}$.

THÉORÈME 4.2. *Soit $\mathcal{V}$ un espace vectoriel sur le corps $\mathcal{F}$. L'algèbre $\mathcal{A}ut\, \mathcal{V}$ est alors un groupe.*

Démonstration. L'ensemble Aut $\mathcal{V}$ d'opérateurs inversibles de l'espace $\mathcal{V}$ est fermé par rapport aux opérations $\cdot$ et ${}^{-1}$. En effet, si φ est un opérateur inversible, φ^{-1} est alors un opérateur inversible, car $\varphi\varphi^{-1} = \varphi^{-1}\varphi = \varepsilon$. En outre, si φ et ψ sont des opérateurs inversibles, leur produit est un opérateur linéaire inversible, car

$$(\varphi\psi)(\psi^{-1}\varphi^{-1}) = \varepsilon \quad \text{et} \quad (\psi^{-1}\varphi^{-1})(\varphi\psi) = \varepsilon.$$

Selon le théorème 2.3, la multiplication d'opérateurs linéaires est associative. L'opérateur identique ε est inversible et est un élé-

ment neutre par rapport à la multiplication, c'est-à-dire que $\varphi\varepsilon = \varepsilon\varphi = \varphi$ pour tout opérateur linéaire φ. Enfin, pour tout opérateur inversible φ se vérifient les égalités $\varphi\varphi^{-1} = \varphi^{-1}\varphi = \varepsilon$. Ainsi, les opérations principales de l'algèbre $\mathcal{A}ut\ \mathcal{V}$ satisfont à tous les axiomes du groupe. Par conséquent, cette algèbre est un groupe. □

THÉORÈME 4.3. *Soit $\mathcal{V}$ un espace vectoriel de dimension $n \neq \{0\}$ sur le corps $\mathcal{F}$. Le groupe $\mathcal{A}ut\ \mathcal{V}$ est alors isomorphe au groupe matriciel linéaire complet $GL(n, \mathcal{F})$.*

Démonstration. Considérons une application bijective

$$\Phi: \mathrm{Aut}\,\mathcal{V} \to GL(n, \mathcal{F}),$$

définie par l'égalité $\Phi(\varphi) = M(\varphi)$, où $M(\varphi)$ est la matrice de l'opérateur linéaire φ relativement à la base fixée de l'espace $\mathcal{V}$. Selon le théorème 3.3, pour tous $\varphi, \psi \in \mathrm{Aut}\,\mathcal{V}$

$$M(\varphi\psi) = M(\varphi)\,M(\psi).$$

Par conséquent, pour tous opérateurs inversibles φ, ψ on a $\Phi(\varphi\psi) = \Phi(\varphi)\,\Phi(\psi)$. Selon le théorème 3.3.1, il s'ensuit que Φ est un homomorphisme. Φ est donc un isomorphisme du groupe $\mathcal{A}ut\ \mathcal{V}$ sur le groupe $GL(n, \mathcal{F})$. □

Exercices

1. Soient φ, ψ des opérateurs linéaires inversibles d'un espace vectoriel. Démontrer que $\varphi\psi$ est un opérateur linéaire inversible et $(\varphi\psi)^{-1} = \psi^{-1}\varphi^{-1}$.

2. Montrer que les opérateurs linéaires φ, ψ d'un espace vectoriel sont inversibles si et seulement si les opérateurs $\varphi\psi$ et $\psi\varphi$ le sont.

3. Soit φ un opérateur inversible de l'espace vectoriel $\mathcal{V}$. Montrer que φ est un isomorphisme de $\mathcal{V}$ sur $\mathcal{V}$.

4. Soient φ, ψ des opérateurs linéaires d'un espace vectoriel $\mathcal{V}$ de dimension finie. Montrer que si $\varphi\psi$ est un opérateur identique de l'espace $\mathcal{V}$, alors φ et ψ sont inversibles.

5. Soient φ, ψ des opérateurs linéaires d'un espace vectoriel. Montrer que si $\mathrm{Ker}\,\varphi = \mathrm{Ker}\,\psi = \{0\}$, alors $\mathrm{Ker}\,(\varphi\psi) = \{0\}$.

6. Soient φ une application linéaire de l'espace vectoriel $\mathcal{U}$ dans l'espace vectoriel $\mathcal{V}$ et ψ une application linéaire de $\mathcal{V}$ dans l'espace vectoriel $\mathcal{W}$. Démontrer que si $\mathrm{Ker}\,\varphi = \{0\}$ et $\mathrm{Ker}\,\psi = \{0'\}$, alors $\mathrm{Ker}\,(\psi\varphi) = \{0\}$.

7. Soient φ un opérateur inversible et ψ un opérateur linéaire quelconque d'un espace vectoriel de dimension finie. Montrer que $\mathrm{rang}\,(\varphi\psi) = \mathrm{rang}\,(\psi\varphi) = \mathrm{rang}\,\psi$.

8. Démontrer que l'opérateur linéaire de l'espace vectoriel de dimension finie $\mathcal{V}$ est inversible si et seulement s'il transforme chaque système de vecteurs linéairement indépendant de l'espace $\mathcal{V}$ en un système de vecteurs linéairement indépendant de cet espace.

9. Soit $\mathcal{H}om(\mathcal{V}, \mathcal{V})$ un espace vectoriel de tous les opérateurs linéaires de l'espace $\mathcal{V}$. Soient φ un opérateur fixé et ψ un opérateur linéaire quelconque de l'espace $\mathcal{V}$. Démontrer que l'application $\psi \mapsto \varphi\psi$ est un opérateur linéaire de l'espace $\mathcal{H}om(\mathcal{V}, \mathcal{V})$. Montrer que l'ensemble $\{\varphi\psi \mid \psi \in \mathrm{Hom}(\mathcal{V}, \mathcal{V})\}$ coïncide avec l'ensemble de tous les opérateurs linéaires de l'espace vectoriel $\mathcal{H}om(\mathcal{V}, \mathcal{V})$ si φ est un opérateur inversible.

§ 5. Vecteurs propres et valeurs propres. Equations caractéristiques

Vecteurs propres et valeurs propres. Soient $\mathscr{V}$ un espace vectoriel sur le corps $\mathscr{F}$ et φ un opérateur linéaire de cet espace.

DÉFINITION. Un vecteur $\mathbf{a} \in V$ est appelé *vecteur propre de l'opérateur* φ si $\mathbf{a} \neq \mathbf{0}$ et le vecteur $\varphi(\mathbf{a})$ est égal au produit d'un scalaire et du vecteur $\mathbf{a}$.

Le scalaire $\lambda \in F$ est appelé *valeur propre de l'opérateur* φ s'il existe un vecteur $\mathbf{a}$ non nul tel que $\varphi(\mathbf{a}) = \lambda\mathbf{a}$.

Si $\mathbf{a}$ est un vecteur propre de l'opérateur φ, il existe alors un scalaire $\lambda \in F$ unique satisfaisant à la condition $\varphi(\mathbf{a}) = \lambda\mathbf{a}$. En effet, si $\mathbf{a} \neq \mathbf{0}$ il s'ensuit de l'égalité $\lambda\mathbf{a} = \lambda_1\mathbf{a}$ que $\lambda = \lambda_1$. Aussi, si $\varphi(\mathbf{a}) = \lambda\mathbf{a}$, dit-on que le vecteur $\mathbf{a}$ est associé à la valeur propre λ.

Exemples 1. Soient $\mathscr{V}$ un espace vectoriel $\neq \{\mathbf{0}\}$ sur le corps $\mathscr{F}$ et λ un scalaire de choix fixé. Définissons l'application φ: $V \to V$, en posant $\varphi(\mathbf{a}) = \lambda\mathbf{a}$ pour tous $\mathbf{a} \in V$. On voit sans peine que φ est un opérateur linéaire de l'espace $\mathscr{V}$; on l'appelle *opérateur d'homothétie de rapport* λ. Le scalaire λ est la valeur propre de l'opérateur φ qui, de plus, est unique. Tout vecteur non nul de l'espace $\mathscr{V}$ est un vecteur propre de l'opérateur φ associé à la valeur propre λ.

2. Soit $\mathscr{V}$ un espace vectoriel des fonctions réelles à une variable définies sur $\mathbf{R}$ et indéfiniment dérivables; $\mathscr{V}$ est l'espace sur le corps des nombres réels $\mathscr{R}$. Notons $\frac{d}{dx}$ l'opérateur de dérivation associant à chaque élément $f \in V$ sa dérivée $\frac{df}{dx}$. On voit sans peine que l'opérateur de dérivation est un opérateur linéaire de l'espace $\mathscr{V}$. Si $\lambda \in \mathbf{R}$, la fonction $e^{\lambda x}$ est alors le vecteur propre de l'opérateur de dérivation, car $\frac{de^{\lambda x}}{dx} = \lambda e^{\lambda x}$. Ainsi, tout nombre réel est la valeur propre de l'opérateur de dérivation.

3. Soient $\mathscr{V}$ un espace vectoriel bidimensionnel sur le corps des nombres réels $\mathscr{R}$, $\mathscr{V} = \mathscr{R}^2$ et $\alpha \in \mathbf{R}$. Notons φ_α l'opérateur de rotation associant à chaque vecteur de l'espace $\mathscr{V}$ un vecteur formant avec le vecteur de départ un angle α. On voit sans peine que φ_α est un opérateur linéaire de l'espace $\mathscr{V}$ qui n'a pas de vecteurs propres si $\alpha \neq k\pi$, où k est un entier.

Notons ε l'opérateur identique de l'espace vectoriel $\mathscr{V}$. Si φ est un opérateur linéaire de l'espace vectoriel $\mathscr{V}$ et λ un scalaire arbitraire, $\lambda \in F$, on constate aisément que $\lambda\varepsilon - \varphi$ est un opérateur linéaire de l'espace $\mathscr{V}$.

PROPOSITION 5.1. *Soient φ un opérateur linéaire de l'espace vectoriel $\mathscr{V}$ et λ la valeur propre de cet opérateur. L'ensemble de tous les vecteurs propres de l'opérateur φ coïncide avec l'ensemble* $\operatorname{Ker}(\lambda\varepsilon - \varphi) \setminus \{\mathbf{0}\}$.

D é m o n s t r a t i o n. Selon la définition du noyau,

$$\mathrm{Ker}\,(\lambda\varepsilon - \varphi) = \{\mathbf{x} \in V \mid (\lambda\varepsilon - \varphi)(\mathbf{x}) = \mathbf{0}\}.$$

Si $\mathbf{a} \in \mathrm{Ker}\,(\lambda\varepsilon - \varphi)\setminus\{\mathbf{0}\}$, alors

$$(\lambda\varepsilon - \varphi)(\mathbf{a}) = \mathbf{0}, \quad \lambda\varepsilon(\mathbf{a}) - \varphi(\mathbf{a}) = \mathbf{0}, \quad \varphi(\mathbf{a}) = \lambda\mathbf{a}.$$

Ainsi, tout vecteur non nul de l'ensemble Ker $(\lambda\varepsilon - \varphi)$ est le vecteur propre de l'opérateur φ.

Soit $\mathbf{b}$ un vecteur propre quelconque de l'opérateur φ associé à λ, c'est-à-dire $\varphi(\mathbf{b}) = \lambda\mathbf{b}$, dans ce cas,

$$\lambda\mathbf{b} - \varphi(\mathbf{b}) = \mathbf{0}, \quad \lambda\varepsilon\mathbf{b} - \varphi(\mathbf{b}) = \mathbf{0}, \quad (\lambda\varepsilon - \varphi)(\mathbf{b}) = \mathbf{0}.$$

Donc, $\mathbf{b} \in \mathrm{Ker}\,(\lambda\varepsilon - \varphi)$, et comme $\mathbf{b} \neq \mathbf{0}$, alors

$$\mathbf{b} \in \mathrm{Ker}\,(\lambda\varepsilon - \varphi)\setminus\{\mathbf{0}\}. \ \square$$

Détermination des vecteurs propres d'un opérateur linéaire. Soient $\mathcal{V}$ un espace vectoriel sur le corps $\mathcal{F}$ avec une base fixée $\mathbf{e}_1, \ldots, \mathbf{e}_n$, φ un opérateur linéaire de cet espace et $A = M(\varphi)$ la matrice de l'opérateur φ relativement à la base fixée, $A = \| a_{ik} \|$.

Pour déterminer les vecteurs propres de l'opérateur φ associés à λ il faut chercher Ker $(\lambda\varepsilon - \varphi)$. Soit $\mathbf{x}$ un vecteur de V; il possède dans la base fixée une colonne de coordonnées $\mathcal{X} = M(\mathbf{x})$:

$$\mathcal{X} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Selon le théorème 2.3, la colonne de coordonnées du vecteur $(\lambda\varepsilon - \varphi)(\mathbf{x})$ est $(\lambda E - A)\,\mathcal{X}$, c'est-à-dire $M((\lambda\varepsilon - \varphi)(\mathbf{x})) = (\lambda E - A)\,\mathcal{X}$. Le vecteur $\mathbf{x} \in \mathrm{Ker}\,(\lambda\varepsilon - \varphi)$ si et seulement si

$$\text{(I)} \quad (\lambda E - A)\mathcal{X} = \mathbf{0}.$$

La condition (I) peut être écrite sous forme d'un système linéaire homogène par rapport aux variables $x_1, \ldots, x_n$:

$$\text{(1)} \quad \begin{array}{l} (\lambda - a_{11})\,x_1 - a_{12}x_2 - \ \ldots\ - a_{1n}x_n = 0; \\ -a_{21}x_1 + (\lambda - a_{22})\,x_2 - \ \ldots\ - a_{2n}x_n = 0; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ -a_{n1}x_1 - a_{n2}x_2 - \ \ldots\ + (\lambda - a_{nn})\,x_n = 0. \end{array}$$

Le vecteur $\mathbf{x} \in V$ est un vecteur propre de l'opérateur φ associé à la valeur propre λ si et seulement si la ligne de coordonnées $(x_1, \ldots, x_n)$ du vecteur $\mathbf{x}$ est une solution non nulle du système linéaire homogène (1). On a ainsi démontré la proposition suivante.

PROPOSITION 5.2. *Soient φ un opérateur linéaire de l'espace vectoriel $\mathcal{V}$ avec base fixée et $M(\varphi) = A$ la matrice de l'opérateur φ relativement à la base fixée. Le vecteur $\mathbf{x}$ est un vecteur propre de l'opérateur φ*

associé à la valeur propre λ *si et seulement si la ligne de coordonnées du vecteur* **x** *est une solution non nulle du système* (1).

Equation caractéristique. Soit $\mathcal{V} = \mathcal{F}^n$ un espace des vecteurs colonnes arithmétiques de dimension n sur le corps $\mathcal{F}$. Soit A la matrice $n \times n$ fixée associée à $\mathcal{F}$. Considérons l'application $\psi : X \to AX$ pour $X \in \mathcal{F}^n$. On vérifie aisément que ψ est un opérateur linéaire de l'espace $\mathcal{V}$.

DÉFINITION. Soit A la matrice $n \times n$ associée au corps $\mathcal{F}$. Le vecteur colonne X est dit *vecteur propre de la matrice* A si X est un vecteur non nul et AX peut être représenté sous forme de produit d'un scalaire et du vecteur X, c'est-à-dire sous forme de $AX = \lambda X$. λ dans ce cas est appelé *valeur propre de la matrice* A.

On voit sans peine que les vecteurs propres et les valeurs propres de l'opérateur linéaire ψ sont des vecteurs propres et des valeurs propres de la matrice A.

THÉORÈME 5.3. *Soit* A *une matrice carrée du type* $n \times n$ *sur le corps* $\mathcal{F}$. *L'élément* λ *de* F *est une valeur propre de la matrice si et seulement si*

$$(1) \quad |\lambda E - A| = 0.$$

D é m o n s t r a t i o n. L'élément λ, $\lambda \in F$, est une valeur propre de la matrice A si et seulement s'il existe un vecteur colonne $X_1 \in F^n$ non nul tel que $AX_1 = \lambda X_1$ et, partant, $(\lambda E - A)X_1 = 0$. Autrement dit, λ est une valeur propre de la matrice A si et seulement si l'équation

$$(2) \quad (A - \lambda E)\, X = 0$$

admet une solution non nulle. L'équation (2) peut être considérée comme la forme matricielle de l'écriture du système de n équations linéaires à n variables avec matrice $(A - \lambda E)$. L'équation (2) a une solution non nulle si et seulement si le déterminant de la matrice $(A - \lambda E)$ est nul. □

COROLLAIRE 5.4. *Un élément* λ *du corps* $\mathcal{F}$ *est une valeur propre de la matrice* A *si et seulement si la matrice* $\lambda E - A$ *est irréversible.*

DÉFINITION. Soit A une matrice carrée du type $n \times n$ sur le corps $\mathcal{F}$. L'équation $|\lambda E - A| = 0$ à variable λ est appelée *équation caractéristique de la matrice* A.

COROLLAIRE 5.5. *Un scalaire* $\lambda \in F$ *est une valeur propre de la matrice carrée* A *(sur* $\mathcal{F}$*) si et seulement si* λ *est une racine de l'équation caractéristique de cette matrice.*

E x e m p l e. Soit $A = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$ une matrice associée au corps des scalaires $\mathcal{R}$. Alors

$$\lambda E - A = \begin{bmatrix} \lambda - 1 & -1 \\ -2 & \lambda - 1 \end{bmatrix}.$$

L'équation

$$\begin{vmatrix} \lambda-1 & -1 \\ -2 & \lambda-1 \end{vmatrix} = 0 \quad \text{ou} \quad (\lambda-1)^2-2=0$$

est l'équation caractéristique de la matrice A. Ses racines $\lambda_1 = 1 + \sqrt{2}$, $\lambda_2 = 1 - \sqrt{2}$ sont les valeurs propres de la matrice A.

PROPOSITION 5.6. *Soient A et B des matrices $n \times n$ semblables sur le corps des scalaires $\mathcal{F}$. Alors $|\lambda E - A| = |\lambda E - B|$ et les équations caractéristiques de ces matrices coïncident.*

Démonstration. Vu que A et B sont semblables, il existe une matrice inversible T sur $\mathcal{F}$ telle que $A = T^{-1}BT$, donc,

$$\lambda E - A = \lambda E - T^{-1}BT = T^{-1}(\lambda E - B)\, T;$$

par conséquent,

$$|\lambda E - A| = |T^{-1}|\,|\lambda E - B|\,|T|.$$

Comme $|T^{-1}|\,|T| = |T^{-1}T| = |E| = 1$, on a $|\lambda E - A| = |\lambda E - B|$. Il s'ensuit que les équations caractéristiques

$$|\lambda E - A| = 0 \quad \text{et} \quad |\lambda E - B| = 0$$

des matrices A et B coïncident. □

DÉFINITION. Soient φ un opérateur linéaire de l'espace vectoriel $\mathcal{V}$ de dimension finie $\neq \{0\}$ et $M(\varphi)$ sa matrice relativement à une base quelconque. L'équation $|\lambda E - M(\varphi)| = 0$ est appelée *équation caractéristique de l'opérateur* φ.

Opérateurs linéaires à spectre simple. Etudions les opérateurs linéaires d'un espace vectoriel de dimension n possédant n valeurs propres différentes.

THÉORÈME 5.7. *Si les vecteurs propres $\mathbf{a}_1, \ldots, \mathbf{a}_m$ de l'opérateur linéaire possèdent des valeurs propres différentes, le système $\mathbf{a}_1, \ldots, \mathbf{a}_m$ est alors linéairement indépendant.*

DÉMONSTRATION. Soient φ un opérateur linéaire de l'espace vectoriel $\mathcal{V}$ et $\mathbf{a}_1, \ldots, \mathbf{a}_m$ ses vecteurs propres associés à de différentes valeurs propres, c'est-à-dire

(1) $\quad \varphi(\mathbf{a}_1) = \lambda_1\mathbf{a}_1, \ldots, \varphi(\mathbf{a}_m) = \lambda_m\mathbf{a}_m$

et

(2) $\quad \lambda_i \neq \lambda_k \quad$ pour $\quad i \neq k.$

La démonstration est effectuée par récurrence sur le nombre m. Vu que tout vecteur propre est différent du vecteur nul, le théorème est vrai pour $m = 1$. En admettant que le théorème est vrai pour $m - 1$ vecteurs, démontrons qu'il est vrai pour m vecteurs. Il faut démontrer que pour tous $\alpha_1, \ldots, \alpha_m \in F$ il s'ensuit de l'égalité

(3) $\quad \alpha_1\mathbf{a}_1 + \ldots + \alpha_m\mathbf{a}_m = 0$

les égalités

(4) $\alpha_1 = 0, \ldots, \alpha_m = 0.$

φ étant un opérateur linéaire il s'ensuit de (3) l'égalité $\alpha_1\varphi(\mathbf{a}_1) + \ldots$ $\ldots + \alpha_m\varphi(\mathbf{a}_m) = \mathbf{0}$ et, en vertu de (1), on a

(5) $\alpha_1\lambda_1\mathbf{a}_1 + \ldots + \alpha_m\lambda_m\mathbf{a}_m = \mathbf{0}.$

Ajoutons aux deux membres de l'égalité (5) les parties correspondantes de l'égalité (3) multipliées par $(-\lambda_m)$, il vient alors

(6) $\alpha_1(\lambda_1 - \lambda_m)\mathbf{a}_1 + \ldots + \alpha_{m-1}(\lambda_{m-1} - \lambda_m)\mathbf{a}_{m-1} = \mathbf{0}.$

Selon l'hypothèse de récurrence, le système des vecteurs propres $\mathbf{a}_1, \ldots, \mathbf{a}_{m-1}$ est linéairement indépendant. Aussi déduit-on de (6) les égalités

$$\alpha_1(\lambda_1 - \lambda_m) = 0, \ldots, \alpha_{m-1}(\lambda_{m-1} - \lambda_m) = 0.$$

En raison de (2) on en tire

(7) $\alpha_1 = 0, \ldots, \alpha_{m-1} = 0.$

En vertu de (3) et (7) $\alpha_m\mathbf{a}_m = \mathbf{0}$, de plus, $\mathbf{a}_m \neq \mathbf{0}$; par conséquent, $\alpha_m = 0$.

On a ainsi démontré que de (3) s'ensuit (4), c'est-à-dire que le système $\mathbf{a}_1, \ldots, \mathbf{a}_m$ est linéairement indépendant. □

Définition. L'opérateur linéaire d'un espace vectoriel de dimension n $(n > 0)$ possédant n valeurs propres différentes est appelé *opérateur à spectre simple*; le jeu de toutes les valeurs propres d'un opérateur est appelé *spectre de l'opérateur*.

Proposition 5.8. *Soit φ un opérateur linéaire de l'espace vectoriel $\mathscr{V}$ de dimension n à spectre simple $\{\lambda_1, \ldots, \lambda_n\}$. Soient $\mathbf{e}_1, \ldots, \mathbf{e}_n$ les vecteurs propres de l'opérateur φ associés respectivement à $\lambda_1, \ldots, \lambda_n$. Le système $\mathbf{e}_1, \ldots, \mathbf{e}_n$ est alors une base de l'espace $\mathscr{V}$.*

Démonstration. Par hypothèse, le spectre $\lambda_1, \ldots, \lambda_n$ de l'opérateur φ est composé des scalaires différents deux à deux. En raison du théorème 5.7, en découle que le système des vecteurs propres $\mathbf{e}_1, \ldots, \mathbf{e}_n$ est linéairement indépendant. Selon le corollaire 7.3.4 il s'ensuit que le système $\mathbf{e}_1, \ldots, \mathbf{e}_n$ est une base de l'espace $\mathscr{V}$. □

Théorème 5.9. *Soient φ un opérateur linéaire de l'espace vectoriel $\mathscr{V}$ de dimension n à spectre simple $\lambda_1, \ldots, \lambda_n$ et $\mathbf{e}_1, \ldots, \mathbf{e}_n$ des vecteurs propres de l'opérateur φ associés respectivement aux valeurs propres $\lambda_1, \ldots, \lambda_n$. La matrice diagonale*

(1) $$\begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}$$

est alors une matrice de l'opérateur φ *relativement à la base* $\mathbf{e}_1, \ldots, \mathbf{e}_n$ *et pour tout vecteur* $\mathbf{x} = x_1\mathbf{e}_1 + \ldots + x_n\mathbf{e}_n$ *de l'espace* $\mathscr{V}$

(2) $\varphi(\mathbf{x}) = \lambda_1 x_1 \mathbf{e}_1 + \ldots + \lambda_n x_n \mathbf{e}_n.$

D é m o n s t r a t i o n. Par hypothèse,

(3) $\varphi(\mathbf{e}_1) = \lambda_1\mathbf{e}_1, \ldots, \varphi(\mathbf{e}_n) = \lambda_n\mathbf{e}_n.$

Ces égalités montrent que la matrice diagonale (1) est une matrice de l'opérateur φ relativement à la base $\mathbf{e}_1, \ldots, \mathbf{e}_n$. Ensuite, si $\mathbf{x} \in V$ et $\mathbf{x} = x_1\mathbf{e}_1 + \ldots + x_n\mathbf{e}_n$, en raison de la linéarité de l'opérateur φ, on a $\varphi(\mathbf{x}) = x_1\varphi(\mathbf{e}_1) + \ldots + x_n\varphi(\mathbf{e}_n)$. En vertu de (3), il s'ensuit les égalités (2). □

Condition de similitude d'une matrice à une matrice diagonale.

THÉORÈME 5.10. *Soient A une matrice* $n \times n$ *sur le corps* $\mathscr{F}$ *possédant n vecteurs propres linéairement indépendants et T la matrice dont les colonnes sont des vecteurs propres linéairement indépendants de la matrice A. La matrice* $T^{-1}AT$ *est alors diagonale et les éléments de sa diagonale principale sont les valeurs propres de la matrice A.*

D é m o n s t r a t i o n. Soit

$$X_1, \ldots, X_n$$

les vecteurs propres linéairement indépendants de la matrice A associés respectivement à $\lambda_1, \ldots, \lambda_n$, c'est-à-dire

$$AX_1 = \lambda_1 X_1, \ldots, AX_n = \lambda_n X_n.$$

Notons T une telle matrice, de sorte que $T^i = X_i$ pour $i = 1, \ldots, n$, c'est-à-dire

$$T = [X_1, \ldots, X_n].$$

Comme les colonnes de la matrice T sont linéairement indépendantes, cette dernière est inversible. De la définition du produit des matrices, on déduit que

$$AT = [AX_1, \ldots, AX_n];$$

d'où, en raison de (1), il vient

$$AT = [\lambda_1 X_1, \ldots, \lambda_n X_n] = [X_1, \ldots, X_n]\begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix} = T\begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}.$$

On obtient ainsi

$$T^{-1}AT = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}. \square$$

THÉORÈME 5.11. *Si une matrice carrée A d'ordre n est semblable sur le corps $\mathcal{F}$ à une matrice diagonale, la matrice A possède alors n vecteurs propres linéairement indépendants.*

Démonstration. Supposons que la matrice A est semblable sur le corps $\mathcal{F}$ à une matrice diagonale, c'est-à-dire qu'il existe une matrice inversible T telle que

$$(1) \quad T^{-1}AT = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}$$

avec $\lambda_1, \ldots, \lambda_n \in F$. Multiplions à gauche les deux membres de l'égalité (1) par T; il vient alors

$$AT = T \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}.$$

Par conséquent,

$$[AT^1, \ldots, AT^n] = [\lambda_1 T^1, \ldots, \lambda_n T^n],$$

et, par suite,

$$AT^1 = \lambda_1 T^1, \ldots, AT^n = \lambda_n T^n,$$

autrement dit, les colonnes $T^1, \ldots, T^n$ de la matrice T sont des vecteurs propres associés respectivement à $\lambda_1, \ldots, \lambda_n$. Comme la matrice T est inversible, ses colonnes sont linéairement indépendantes (selon le théorème 5.1). $\square$

Exercices

1. Chercher les vecteurs propres et les valeurs propres des matrices suivantes sur le corps des nombres rationnels:

(a) $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$; (b) $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$; (c) $\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$.

2. Soit α un nombre réel non nul. Montrer que la matrice $\begin{bmatrix} 0 & \alpha \\ -\alpha & 0 \end{bmatrix}$ ne possède pas de valeurs propres réelles.

3. Soit α un nombre réel différent de zéro. Chercher les valeurs propres et les vecteurs propres sur le corps des nombres complexes de la matrice $\begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}$.

4. Chercher les vecteurs propres et les valeurs propres sur le corps des nombres complexes des matrices suivantes:

$$\text{(a)} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}; \quad \text{(b)} \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}; \quad \text{(c)} \begin{bmatrix} 1 & 2 \\ 2 & -2 \end{bmatrix}; \quad \text{(d)} \begin{bmatrix} -1 & -2i \\ 2i & 2 \end{bmatrix}.$$

5. Soit $A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ une matrice sur le corps $\mathcal{F}$. Montrer que le scalaire $\lambda \in F$ est une valeur propre de la matrice A quand $\lambda^2 - (\alpha + \delta)\lambda + (\alpha\delta - - \beta\gamma) = 0$.

6. Démontrer que les nombres réels sont les valeurs propres d'une matrice réelle symétrique.

7. Soit A une matrice carrée. Montrer que la matrice transposée ${}^tA$ possède les mêmes valeurs propres que la matrice A.

8. Montrer que les valeurs propres d'une matrice diagonale sont ses éléments diagonaux.

9. Démontrer que les valeurs propres d'une matrice triangulaire sont ses éléments diagonaux.

10. Demontrer que toutes les valeurs propres d'une matrice carrée A sont différentes de zéro si et seulement si la matrice A est inversible.

11. Soient A une matrice carrée et k tout entier positif. Démontrer que si λ est une valeur propre de la matrice A, λ^k est alors une valeur propre de la matrice A^k.

12. Les valeurs propres d'une matrice inversible A étant connues chercher les valeurs propres de la matrice A^{-1}.

13. Soit λ la valeur propre d'une matrice inversible A. Démontrer que λ^n est une valeur propre de la matrice A^n pour tout n entier.

14. Soit A une matrice carrée sur le corps $\mathcal{F}$:

$$f(\lambda) = \alpha_0 + \alpha_1\lambda + \ldots + \alpha_m\lambda^m, \quad \text{où} \quad \alpha_0, \alpha_1, \ldots, \alpha_m \in F,$$

$$f(A) = \alpha_0 E + \alpha_1 A + \ldots + \alpha_m A^m \ (E \text{ est la matrice unité}).$$

Démontrer que si λ est une valeur propre de la matrice A, alors $f(\lambda)$ est une valeur propre de la matrice $f(A)$. Montrer que tout vecteur propre de la matrice A est un vecteur propre de la matrice $f(A)$.

15. Soient A, B des matrices carrées $n \times n$ sur le corps $\mathcal{F}$, la matrice A étant inversible. Démontrer que les matrices AB et BA possèdent une même équation caractéristique.

16. Chercher la matrice diagonale semblable sur le corps des nombres rationnels à la matrice:

$$\text{(a)} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad \text{(b)} \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}; \quad \text{(c)} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}.$$

17. Chercher la matrice diagonale semblable sur le corps des nombres réels à la matrice:

$$\text{(a)} \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}; \quad \text{(b)} \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}; \quad \text{(c)} \begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix}.$$

18. Chercher la matrice diagonale semblable sur le corps des nombres complexes à la matrice $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.

19. Soit α un nombre réel non entier multiple de π. Démontrer que la matrice $\begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}$ n'est pas semblable à la matrice diagonale réelle.

20. Montrer que toute matrice 2×2 réelle dont le déterminant est négatif est semblable à la matrice diagonale réelle.

21. Soient $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ une matrice sur le corps $\mathcal{F}$ et $a \neq 0$. Démontrer que la matrice A n'est pas semblable à la matrice diagonale.

22. Démontrer que deux matrices diagonales sont semblables si et seulement si elles ne diffèrent que par l'ordre de disposition des éléments diagonaux.

23. Soit A une matrice semblable à la matrice diagonale. Démontrer que la matrice A^n est semblable à la matrice diagonale pour tout entier positif.

24. Chercher toutes les matrices carrées de deuxième ordre sur le corps $\mathcal{C}$ aux valeurs propres 1 et -1.

19—01762

CHAPITRE IX

SYSTÈMES D'INÉGALITÉS LINÉAIRES

§ 1. Systèmes d'inégalités linéaires

Notions élémentaires. Le système de la forme

(1) $\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n \leqslant \gamma_i \qquad (i = 1, \ldots, m),$

où $\alpha_i \in \mathbf{R}$, $\gamma_i \in \mathbf{R}$, est appelé *système d'inégalités linéaires.*

Posons

$$\mathbf{a}_i = (\alpha_{i1}, \ldots, \alpha_{in}) \qquad (i = 1, \ldots, m).$$

Le système (1) peut être écrit sous la *forme vectorielle*:

(2) $\mathbf{a}_i\mathbf{x} \leqslant \gamma_i \qquad (i = 1, \ldots, m),$

où $\mathbf{x} = \begin{bmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_m \end{bmatrix}.$

Désignons par A la matrice composée des coefficients du système (1):

$$A = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{bmatrix}.$$

Le système (1) peut être écrit sous la *forme matricielle*:

(3) $A\mathbf{x} \leqslant \mathbf{c}, \quad$ où $\quad \mathbf{c} = \begin{bmatrix} \gamma_1 \\ \cdot \\ \cdot \\ \cdot \\ \gamma_n \end{bmatrix}.$

Soient $\mathscr{R}^n$ l'espace arithmétique de dimension n sur le corps des nombres réels $\mathscr{R}$ et $\mathbf{R}^n$ son ensemble de base.

Le vecteur de $\mathbf{R}^n$ aux coordonnées $\xi_1, \ldots, \xi_n$ est appelé *solution du système* (1) si

$$\alpha_{i1}\xi_1 + \ldots + \alpha_{in}\xi_n \leqslant \gamma_i \qquad (i = 1, \ldots, n).$$

Le système (1) est dit *compatible* s'il admet au moins une solution.

Le système (1) est dit *incompatible* s'il n'admet pas de solutions.

Le vecteur $(\xi_1, \ldots, \xi_n) \in \mathbf{R}^n$ est dit *non négatif* si $\xi_i \geqslant 0$ pour $i = 1, \ldots, n$. Un vecteur non négatif $\xi_i, \ldots, \xi_n$ est dit *positif* si l'une au moins de ses coordonnées est positive.

L'inégalité

$$(4) \quad \beta_1 x_1 + \ldots + \beta_n x_n \leqslant \gamma$$

est appelée *implication du système* (1) si chaque solution du système (1) est une solution de l'inégalité (4).

L'inégalité de la forme

$$(5) \quad (\lambda_1 \mathbf{a}_1 + \ldots + \lambda_m \mathbf{a}_m)\, \mathbf{x} \leqslant \lambda_1 \gamma_1 + \ldots + \lambda_m \gamma_m,$$

où $\lambda_1 \geqslant 0, \ldots, \lambda_m \geqslant 0$, est appelée *combinaison linéaire non négative d'inégalités du système* (2).

PROPOSITION 1.1. *Toute combinaison linéaire non négative d'inégalités du système* (2) *est une implication de ce système.*

D é m o n s t r a t i o n. Posons que l'inégalité (5) est une combinaison linéaire non négative d'inégalités du système (2). Soit $\xi \in \mathbf{R}^n$ une solution quelconque du système (2),

$$(6) \quad \mathbf{a}_i \xi \leqslant \gamma_i \qquad (i = 1, \ldots, m).$$

En multipliant la i-ième inégalité de (6) par λ_i pour $i = 1, \ldots, m$ et en additionnant ces inégalités, il vient

$$(\lambda_1 \mathbf{a}_1 + \ldots + \lambda_m \mathbf{a}_m)\, \xi \leqslant \lambda_1 \gamma_1 + \ldots + \lambda_m \gamma_m.$$

Ainsi, l'inégalité (5) est l'implication du système (2). □

Systèmes homogènes d'inégalités linéaires et cônes convexes. Soient $\mathcal{T}$ un espace vectoriel arithmétique sur le corps des nombres réels $\mathcal{R}$, $\mathcal{T} = \mathcal{R}^n$ et $\mathbf{a}_1, \ldots, \mathbf{a}_m$ des vecteurs de l'espace $\mathcal{T}$.

Le système

$$(1) \quad \mathbf{a}_i \mathbf{x} \leqslant 0 \qquad (i = 1, \ldots, m)$$

est appelé *système d'inégalités linéaire homogène.*

DEFINITION. Un ensemble non vide de vecteurs de l'espace vectoriel $\mathcal{T}$, fermé par rapport à l'addition et à la multiplication par des scalaires non négatifs (des nombres réels non négatifs) est appelé *cône convexe de l'espace* $\mathcal{T}$.

E x e m p l e s. 1. Soit $\mathbf{a} \in \mathbf{R}^n$, $\mathbf{a} \neq 0$. L'ensemble

$$\{\lambda \mathbf{a} \mid \lambda \geqslant 0,\ \lambda \in \mathbf{R}\}$$

est un cône convexe de l'espace $\mathcal{R}^n$. Ce cône est appelé *demi-droite engendrée par le vecteur* $\mathbf{a}$.

2. L'ensemble de toutes les combinaisons non négatives du système des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$ de l'espace $\mathcal{R}^n$ est un cône convexe de cet espace; on le notera $L^+(\mathbf{a}_1, \ldots, \mathbf{a}_m)$.

3. Soit $\mathscr{V} = \mathscr{R}^n$, $\mathscr{L}$ étant un sous-espace de l'espace $\mathscr{V}$ et L son ensemble de base. Alors, L est un cône convexe de l'espace $\mathscr{V}$.

4. L'ensemble de toutes les solutions non négatives d'un système d'inégalités linéaire homogène (1) est un cône convexe de l'espace $\mathscr{V}$.

5. Soit $\mathbf{a} \in \mathbf{R}^n$, $\mathbf{a} \neq 0$. L'ensemble de toutes les solutions de l'inégalité $\mathbf{ax} \leqslant 0$ est un cône convexe de l'espace $\mathscr{V}$. Ce cône est appelé *sous-espace de l'espace $\mathscr{V}$ défini par le vecteur* $\mathbf{a}$.

PROPOSITION 1.2. *Un ensemble de toutes les solutions du système linéaire homogène* (1) *est un cône convexe d'un espace vectoriel $\mathscr{V}$.*

La démonstration de cette proposition est laissée au soin du lecteur.

COROLLAIRE 1.3. *Si $\mathbf{a}_1, \ldots, \mathbf{a}_m$ sont des vecteurs non nuls, alors le cône de toutes les solutions du système linéaire homogène* (1) *est une intersection de m sous-espaces de l'espace $\mathscr{V}$ définis par les vecteurs* $\mathbf{a}_1, \ldots, \mathbf{a}_m$.

Implications d'un système homogène d'inégalités linéaires. Pour démontrer le théorème de Minkowski il nous faut deux lemmes.

LEMME 1.4. *Si*

$$\mathbf{b} \notin L(\mathbf{a}_1, \ldots, \mathbf{a}_m), \tag{3}$$

alors l'inégalité

$$\mathbf{bx} \leqslant 0 \tag{2}$$

n'est pas une implication du système

$$\mathbf{a}_i\mathbf{x} \leqslant 0 \qquad (i = 1, \ldots, m). \tag{1}$$

D é m o n s t r a t i o n. Le rang du système des vecteurs $\mathbf{a}_1, \ldots$ $\ldots, \mathbf{a}_m$ sera noté r. Supposons qu'est satisfaite la condition (3), alors

$$\operatorname{rang}\{\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}\} = \operatorname{rang}\{\mathbf{a}_1, \ldots, \mathbf{a}_m\} + 1 = r + 1. \tag{4}$$

Soient

$$\mathbf{a}_i = (\alpha_{i1}, \ldots, \alpha_{in}) \qquad (i = 1, \ldots, m);$$
$$\mathbf{b} = (\beta_1, \ldots, \beta_n).$$

Considérons le système d'équations linéaires

$$\begin{aligned} &\alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = 0,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ &\alpha_{m1}x_1 + \ldots + \alpha_{mn}x_n = 0,\\ &\beta_1 x_1 + \ldots + \beta_n x_n = 1. \end{aligned} \tag{5}$$

Sur la base de (4) on conclut que les rangs des matrices fondamentale et complète du système (5) valent $r + 1$. Par conséquent, le systè-

me (5) est compatible. Aussi existe-t-il un vecteur ξ tel que

$$\begin{matrix} \mathbf{a}_i\xi = 0 \\ \mathbf{b}\xi = 1 \end{matrix} \qquad (i = 1, \ldots, m).$$

Le vecteur ξ est la solution du système (1) qui ne satisfait pas à (2). Ainsi, l'inégalité (2) n'est pas une implication du système (1). □

Corollaire 1.5. *Si l'inégalité* (2) *est l'implication du système* (1), *alors*

$$\mathbf{b} \in L(\mathbf{a}_1, \ldots, \mathbf{a}_m).$$

Selon la loi de contraposition cette affirmation est équipotente au lemme 1.4.

Lemme 1.6. *Soient l'inégalité*

(2) $\quad \mathbf{cx} \leqslant 0$

une implication du système

(1) $\quad \mathbf{a}_i\mathbf{x} \leqslant 0 \qquad (i = 1, \ldots, m)$

et

(3) $\quad \mathbf{c} = \lambda_1\mathbf{a}_1 + \ldots + \lambda_{m-1}\mathbf{a}_{m-1} + \lambda_m\mathbf{a}_m,$

$$\lambda_1, \ldots, \lambda_{m-1} \geqslant 0, \ \lambda_m \leqslant 0.$$

Alors, l'inégalité (2) *est une implication du système*

(4) $\quad \mathbf{a}_i\mathbf{x} \leqslant 0 \qquad (i = 1, \ldots, m-1).$

Démonstration. Considérons le système

(I) $\quad \mathbf{a}_1\mathbf{x} \leqslant 0, \ldots, \mathbf{a}_{m-1}\mathbf{x} \leqslant 0, \qquad (-\mathbf{a}_m)\,\mathbf{x} \leqslant 0.$

Le vecteur $\mathbf{c}$, en vertu de (3), est une combinaison linéaire non négative des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_{m-1}, (-\mathbf{a}_m)$,

(II) $\quad \mathbf{c} = \lambda_1\mathbf{a}_1 + \ldots + \lambda_{m-1}\mathbf{a}_{m-1} + (-\lambda_m)(-\mathbf{a}_m).$

En vertu de la proposition 1.1, il s'ensuit que (2) est une implication du système (II):

(5) $\quad (\mathrm{II}) \rightarrow (2).$

Il nous faut démontrer que toute solution ξ du système (4) est une solution de l'inégalité (2). Deux cas sont possibles: $\mathbf{a}_m\xi \leqslant 0$ ou $(-\mathbf{a}_m)\xi \leqslant 0$. Si $\mathbf{a}_m\xi \leqslant 0$, alors ξ est une solution du système (1) et, par conséquent, par hypothèse, ξ est une solution de l'inégalité (2). Si, par contre, $-\mathbf{a}_m\xi \leqslant 0$, alors ξ est une solution du système (1'); par conséquent, en raison de (4), c'est également une solution de l'inégalité (2). Bref, toute solution de (4) est une solution de l'inégalité (2). □

Théorème de Minkowski. En théorie des inégalités linéaires un des théorèmes essentiels est le suivant.

THÉORÈME 1.7. *Soit l'inégalité*

(2) $\mathbf{b}\mathbf{x} \leqslant 0$

considérée comme une implication du système

(1) $\mathbf{a}_i\mathbf{x} \leqslant 0 \qquad (i = 1, \ldots, m).$

Alors, $\mathbf{b} \in L^+(\mathbf{a}_1, \ldots, \mathbf{a}_m)$.

Démonstration*) (conduite par récurrence sur m). Le théorème est vrai pour $m = 1$. En effet, posons $\mathbf{b} \neq \mathbf{0}$. Par hypothèse, l'inégalité $\mathbf{b}\mathbf{x} \leqslant 0$ est l'implication de l'inégalité $\mathbf{a}_1\mathbf{x} \leqslant 0$. Selon le corollaire 1.5, $\mathbf{b} = \lambda\mathbf{a}_1$, où $\lambda \in \mathbf{R}$. Comme $\mathbf{b} \neq \mathbf{0}$, on a $\lambda \neq 0$, $\mathbf{a}_1 \neq \mathbf{0}$ et $\mathbf{a}_1\mathbf{a}_1 > 0$. Donc le vecteur $(-\mathbf{a}_1)$ est une solution de l'inégalité $\mathbf{a}_1\mathbf{x} \leqslant 0$ et, par hypothèse, une solution de l'inégalité (2), c'est-à-dire $\lambda\mathbf{a}_1(-\mathbf{a}_1) \leqslant 0$. Par conséquent, $\lambda > 0$. Le théorème est apparemment vrai pour $\mathbf{b} = \mathbf{0}$.

Supposons que le théorème se vérifie quand le système est composé de $m - 1$ inégalités. Etant donné que (1) → (2), en raison du corollaire 1.5, $\mathbf{b} \in L(\mathbf{a}_1, \ldots, \mathbf{a}_m)$. Parmi les représentations du vecteur $\mathbf{b}$ il y a une représentation où le nombre des coefficients non négatifs est le plus grand. Soit

(3) $\mathbf{b} = \lambda_1\mathbf{a}_1 + \ldots + \lambda_m\mathbf{a}_m$

une de ces représentations. Soit s le nombre des coefficients non négatifs dans (3), $s \leqslant m$. Il faut démontrer que $s = m$. Posons que

(4) $s < m$.

Par convention, les coefficients $\lambda_1, \ldots, \lambda_s$ ne sont pas négatifs. Considérons le vecteur

$$\mathbf{c} = \sum_{1 \leqslant i \leqslant s} \lambda_i\mathbf{a}_i + \lambda_m\mathbf{a}_m ;$$

alors,

(5) $\mathbf{b} - \mathbf{c} = \sum_{s<k<m} \lambda_k\mathbf{a}_k.$

Soit M un ensemble de toutes les solutions du système (1) et ξ un vecteur quelconque de M, alors $\mathbf{a}_k\xi \leqslant 0$ et $\lambda_k(\mathbf{a}_k\xi) \geqslant 0$ si $s < k < m$; par conséquent,

(6) $(\mathbf{b} - \mathbf{c})\xi = \sum_{s<k<m} \lambda_k\mathbf{a}_k\xi \geqslant 0.$

---

*) La démonstration figure dans l'ouvrage de S. N. Tchernikov « Théorèmes fondamentaux de la théorie des inégalités linéaires » (С. Н. Черников, « Об основных теоремах теории линейных неравенств ». Сибирск. матем. ж., 1964, № 5).

En outre, par hypothèse, $\mathbf{b}\xi \leqslant 0$; donc,

(7) $\mathbf{c}\xi + (\mathbf{b} - \mathbf{c})\xi \leqslant 0.$

Sur la base de (6) et (7) on conclut que $\mathbf{c}\xi \leqslant 0$ pour tout ξ de M, c'est-à-dire que l'inégalité $\mathbf{cx} \leqslant 0$ est une implication du système (1).

Selon le lemme 1.6, il en découle que l'inégalité $\mathbf{cx} \leqslant 0$ est une implication du système

$$\mathbf{a}_i\mathbf{x} \leqslant 0 \qquad (i = 1, \ldots, m - 1),$$

composé de $m - 1$ inégalités. Selon l'hypothèse de récurrence, $\mathbf{c} \in L^+ (\mathbf{a}_1, \ldots, \mathbf{a}_{m-1})$, c'est-à-dire $\mathbf{c}$ peut être représenté sous forme de

(8) $\mathbf{c} = \gamma_1\mathbf{a}_1 + \ldots + \gamma_{m-1}\mathbf{a}_{m-1}, \quad$ où $\quad \gamma_1, \ldots, \gamma_{m-1} \geqslant 0.$

En raison de (5) et (8)

$$\mathbf{b} = \sum_{1 \leqslant i \leqslant s} \gamma_i \mathbf{a}_i + \sum_{s < k < m} (\gamma_k + \lambda_k)\, \mathbf{a}_k + 0 \cdot \mathbf{a}_m.$$

En cette représentation du vecteur $\mathbf{b}$ le nombre des coefficients non négatifs est supérieur à s. Cela contredit l'hypothèse que la représentation (3) du vecteur $\mathbf{b}$ renferme le plus grand nombre des coefficients non négatifs. On a abouti à une contradiction en admettant que $s < m$. Ainsi, ce cas est impossible. Par conséquent, $s = m$, c'est-à-dire (3) est la représentation cherchée du vecteur $\mathbf{b}$ sous forme d'une combinaison non négative des vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_m$. □

Critère d'incompatibilité d'un système d'inégalités linéaires. Passons à l'étude des systèmes d'inégalités linéaires non homogènes.

THÉORÈME 1.8. *Le système d'inégalités*

(1) $\mathbf{a}_i\mathbf{x} \leqslant \gamma_i \qquad (i = 1, \ldots, m)$

est incompatible si et seulement s'il existe des nombres réels $\lambda_1, \ldots, \lambda_m$ *satisfaisant aux conditions*

(2) $$\begin{aligned} \lambda_1\mathbf{a}_1 + \ldots + \lambda_m\mathbf{a}_m &= \mathbf{0} \\ \lambda_1\gamma_1 + \ldots + \lambda_m\gamma_m &< 0 \end{aligned} \qquad (\lambda_1 \geqslant 0, \ldots, \lambda_m \geqslant 0).$$

D é m o n s t r a t i o n. Supposons que le système (1) est incompatible et démontrons qu'il existe les nombres réels satisfaisant aux conditions (2). Soit

(3) $\mathbf{a}_i = (\alpha_{i1}, \ldots, \alpha_{in}) \qquad (i = 1, \ldots, m).$

Considérons un système d'inégalités homogène

(4) $\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n - \gamma_i x_{n+1} \leqslant 0 \qquad (i = 1, \ldots, m)$

aux variables $x_1, \ldots, x_n, x_{n+1}$. L'inégalité

5) $0 \cdot x_1 + \ldots + 0 \cdot x_n + x_{n+1} \leqslant 0$

est une implication du système (4). En effet, si $(\xi_1, \ldots, \xi_n, \xi_{n+1})$ est une solution arbitraire du système (4), alors

(6) $\xi_{n+1} \leqslant 0,$

car pour $\xi_{n+1} > 0$ le vecteur $(\xi_1\xi_{n+1}^{-1}, \ldots, \xi_n\xi_{n+1}^{-1}, 1)$ serait une solution du système (4), tandis que le vecteur $(\xi_1\xi_{n+1}^{-1}, \ldots, \xi_n\xi_{n+1}^{-1})$ une solution du système de départ (1), ce qui contredirait l'hypothèse de l'incompatibilité de ce système.

Comme l'inégalité (5) est une implication du système (4), selon le théorème de Minkowski, le vecteur $(0, \ldots, 0, 1)$ peut être représenté sous forme d'une combinaison linéaire non négative des vecteurs

$$(\alpha_{11}, \ \ldots, \alpha_{1n}, \ -\gamma_1),$$
$$\ldots\ldots\ldots\ldots$$
$$(\alpha_{m1}, \ \ldots, \alpha_{mn}, \ -\gamma_m),$$

autrement dit, il existe des nombres réels $\lambda_1, \ldots, \lambda_m$ tels que

$$\begin{aligned} &\lambda_1\alpha_{11} + \ldots + \lambda_m\alpha_{m1} = 0, \\ &\ldots\ldots\ldots\ldots \\ &\lambda_1\alpha_{1n} + \ldots + \lambda_m\alpha_{mn} = 0, \qquad \lambda_1 \geqslant 0, \ \ldots, \ \lambda_m \geqslant 0, \\ &\lambda_1(-\gamma_1) + \ldots + \lambda_m(-\gamma_m) = 1. \end{aligned}$$

En raison de (3), il s'ensuit que

$$\begin{aligned} &\lambda_1\mathbf{a}_1 + \ldots + \lambda_m\mathbf{a}_m = \mathbf{0}, \\ &\lambda_1\gamma_1 + \ldots + \lambda_m\gamma_m < 0, \end{aligned} \qquad \lambda_1 \geqslant 0, \ \ldots, \ \lambda_m \geqslant 0,$$

c'est-à-dire les conditions (2) sont satisfaites.

Supposons maintenant qu'il existe des nombres réels $\lambda_1, \ldots, \lambda_m$ satisfaisant aux conditions (2) et démontrons que le système (1) est incompatible. Considérons l'inégalité

(7) $(\lambda_1\mathbf{a}_1 + \ldots + \lambda_m\mathbf{a}_m)\,\mathbf{x} \leqslant \lambda_1\gamma_1 + \ldots + \lambda_m\gamma_m,$

constituant une combinaison linéaire non négative d'inégalités du système (1). Selon la proposition 1.1, cette inégalité est une implication du système (1). En raison de (2), l'inégalité (7) peut être écrite sous forme

$$\mathbf{0}\cdot\mathbf{x} < 0.$$

Cette inégalité n'a pas de solutions et est une implication du système (1), aussi le système (1) est-il incompatible. □

Soit $\mathbf{a}_i = (\alpha_{i1}, \ldots, \alpha_{in})$ pour $i = 1, \ldots, m$,

$$A = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \cdot & \cdot\cdot\cdot & \cdot \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{bmatrix}, \qquad {}^tA = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{m1} \\ \cdot & \cdot\cdot\cdot & \cdot \\ \alpha_{1n} & \ldots & \alpha_{mn} \end{bmatrix}.$$

THÉORÈME 1.9. *L'inégalité*

(2) $\mathbf{bx} \leqslant 0$

est une implication de l'inégalité

(1) $A\mathbf{x} \leqslant 0$

si et seulement si le système

(3) ${}^tA\mathbf{y} = \mathbf{b}, \qquad \mathbf{y} \geqslant 0,$

est compatible.

Le théorème 1.9 découle directement de la proposition 1.1 et du théorème 1.8.

THÉORÈME 1.10. *Un système*

$$A\mathbf{x} + \mathbf{b} = 0, \qquad \mathbf{x} \geqslant 0$$

(où $\mathbf{b}$ *est une colonne) est compatible si et seulement si pour tout* $\mathbf{y}$ ${}^tA\mathbf{y} \geqslant 0 \to {}^t\mathbf{b}\mathbf{y} \leqslant 0$.

En remplaçant dans le théorème 1.9 A, ${}^tA$, $\mathbf{b}$, ${}^t\mathbf{b}$, $\mathbf{x}$, $\mathbf{y}$ respectivement par $-{}^tA$, $-A$, ${}^t\mathbf{b}$, $\mathbf{b}$, $\mathbf{y}$, $\mathbf{x}$ on se convaincra que le théorème 1.10 n'est qu'une autre expression du théorème 1.9.

Solutions non négatives d'un système d'équations linéaires et d'un système d'inéquations linéaires. Le système d'équations linéaires

(1*) $\alpha_{i1}x_1 + \ldots + \alpha_{in}x_n + \beta_i = 0 \qquad (i = 1, \ldots, m)$

peut être écrit sous forme matricielle

$$A\mathbf{x} + \mathbf{b} = 0,$$

où $A = \| \alpha_{ik} \|$ est une matrice $m \times n$ et $\mathbf{b} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix}$.

Dans l'étude des problèmes de programmation linéaire on est obligé de rechercher les conditions pour lesquelles le système (1*) admet au moins une solution non négative. Cette recherche revient à étudier la compatibilité du système

(1) $A\mathbf{x} + \mathbf{b} = 0, \qquad \mathbf{x} \geqslant 0.$

THÉORÈME 1.11. *Le système* (1) *est compatible si et seulement si est incompatible le système*

(2) ${}^tA\mathbf{y} \geqslant 0, \qquad {}^t\mathbf{b}\mathbf{y} > 0.$

D é m o n s t r a t i o n. Selon le théorème 1.10, le système (1) est compatible si et seulement si

(3) ${}^t\forall\mathbf{y}\ ({}^tA\mathbf{y} \geqslant 0 \to {}^t\mathbf{b}\mathbf{y} \leqslant 0).$

On voit sans peine que

$$\forall \mathbf{y}\,({}^t A\mathbf{y} \geqslant \mathbf{0} \to {}^t\mathbf{b}\mathbf{y} \leqslant 0) \leftrightarrow \forall \mathbf{y}\,(\neg\,({}^t A\mathbf{y} \geqslant \mathbf{0}) \vee ({}^t\mathbf{b}\mathbf{y} \leqslant 0)),$$
$$\leftrightarrow \forall \mathbf{y}\,\neg\,({}^t A(\mathbf{y}) \geqslant \mathbf{0} \wedge {}^t\mathbf{b}\mathbf{y} > 0).$$

Ainsi, le système (1) est compatible si et seulement si pour chaque $\mathbf{y}$

$$\neg\,({}^t A\mathbf{y} \geqslant \mathbf{0} \wedge {}^t\mathbf{b}\mathbf{y} > 0).$$

Par conséquent, le système (1) est compatible si et seulement si est incompatible le système (2). □

Théorème 1.12. *Le système*

(1) $\quad A\mathbf{x} + \mathbf{b} \leqslant \mathbf{0}, \qquad \mathbf{x} \geqslant \mathbf{0},$

est compatible si et seulement si est incompatible le système

(2) $\quad {}^t A\mathbf{y} \geqslant \mathbf{0}, \qquad {}^t\mathbf{b}\mathbf{y} > 0, \qquad \mathbf{y} \geqslant \mathbf{0}.$

Démonstration. Soient A une matrice $m \times n$ et $\mathbf{z} = \begin{bmatrix} z_1 \\ \vdots \\ z_m \end{bmatrix}$. On voit aisément que le système (1) est compatible si et seulement si est compatible le système

(1′) $\quad A\mathbf{x} + \mathbf{z} + \mathbf{b} = \mathbf{0}, \qquad \mathbf{x} \geqslant \mathbf{0}, \qquad \mathbf{z} \geqslant \mathbf{0}.$

E étant une matrice $m \times m$ unité, on a

$$A\mathbf{x} + \mathbf{z} + \mathbf{b} = A\mathbf{x} + E\mathbf{z} + \mathbf{b} = [A \mid E] \begin{bmatrix} \mathbf{x} \\ \mathbf{z} \end{bmatrix} + \mathbf{b}.$$

Aussi le système (1) peut-il être écrit sous forme

$$[A|E] \begin{bmatrix} \mathbf{x} \\ \mathbf{z} \end{bmatrix} + \mathbf{b} = \mathbf{0}, \qquad \begin{bmatrix} \mathbf{x} \\ \mathbf{z} \end{bmatrix} \geqslant \mathbf{0}.$$

Selon le théorème 1.11, le système (1′) est compatible si et seulement si le système

$$\begin{bmatrix} {}^t A \\ E \end{bmatrix} \mathbf{y} \geqslant \mathbf{0}, \qquad {}^t\mathbf{b}\mathbf{y} > 0,$$

est incompatible, c'est-à-dire qu'est incompatible le système

$${}^t A\mathbf{y} \geqslant \mathbf{0}, \qquad \mathbf{y} \geqslant \mathbf{0}, \qquad {}^t\mathbf{b}\mathbf{y} > 0.$$

Par conséquent, le système (1) est compatible si et seulement si est incompatible le système (2). □

Exercices

1. Démontrer que tout système de n inégalités linéaires homogènes à n variables admet des solutions non nulles.
2. Démontrer que l'inégalité $A\mathbf{x} \leqslant 0$ admet des solutions non nulles si et seulement si les solutions non nulles vérifient l'inégalité ${}^tA\mathbf{y} \leqslant 0$.
3. Démontrer que tout polyèdre convexe constitue un ensemble de toutes les solutions d'un certain système d'inégalités linéaires.
4. Montrer qu'un ensemble de toutes les solutions d'un système compatible d'inégalités linéaires peut être assimilé à une somme d'un polyèdre convexe et d'un cône convexe engendré par un ensemble fini de vecteurs.

§ 2. Problèmes standard et canoniques de la programmation linéaire. Théorèmes de dualité

Problèmes standard et canoniques. Partout plus loin A est une matrice $m \times n$ sur le corps des nombres réels $\mathscr{R}$:

$$A = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ & \vdots & \\ \alpha_{m1} & \dots & \alpha_{mn} \end{bmatrix},$$

$\mathbf{b}$ et $\mathbf{c}$ étant respectivement des vecteurs colonnes de dimensions m et n sur $\mathscr{R}$:

$$\mathbf{b} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix}, \quad \mathbf{c} = \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{bmatrix} \quad \text{et} \quad {}^t\mathbf{b} = [\beta_1, \dots, \beta_m],$$

$${}^t\mathbf{c} = [\gamma_1, \dots, \gamma_n].$$

La forme linéaire $\gamma_1 y_1 + \dots + \gamma_n y_n$ s'écrira comme un produit de la ligne ${}^t\mathbf{c}$ et de la colonne $\mathbf{y} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$, c'est-à-dire

$${}^t\mathbf{c}\mathbf{y} = \gamma_1 y_1 + \dots + \gamma_n y_n.$$

La forme linéaire $\beta_1 z_1 + \dots + \beta_m z_m$ s'écrira comme un produit de la ligne ${}^t\mathbf{b}$ par la colonne $\mathbf{z} = \begin{bmatrix} z_1 \\ \vdots \\ z_m \end{bmatrix}$;

$${}^t\mathbf{b}\mathbf{z} = \beta_1 z_1 + \dots + \beta_m z_m.$$

Les principaux problèmes de programmation linéaire se ramènent aux problèmes standard et canoniques de minimum et de maximum.

Problème standard de minimisation

S. *Chercher la solution du système*

$$(1) \quad \begin{aligned} &\alpha_{i1}y_1 + \ldots + \alpha_{in}y_n + \beta_i \leqslant 0 \qquad (i = 1, \ldots, m); \\ &y_1 \geqslant 0, \ldots, y_n \geqslant 0, \end{aligned}$$

minimisant la forme linéaire $\gamma_1 y_1 + \ldots + \gamma_n y_n$.

Problème standard de maximisation

S*. *Chercher la solution du système*

$$(2) \quad \begin{aligned} &\alpha_{1k}z_1 + \ldots + \alpha_{mk}z_m + \gamma_k \geqslant 0, \\ &z_1 \geqslant 0, \ldots, z_m \geqslant 0, \end{aligned}$$

maximisant la forme linéaire $\beta_1 z_1 + \ldots + \beta_m z_m$.

Les conditions (1) et (2) sont appelées *contraintes linéaires* des problèmes S et S* respectivement. Les problèmes S et S* sont dits *duals l'un de l'autre.*

Sous forme matricielle ces problèmes sont énoncés de la façon suivante:

S. *Chercher la solution du système*

$$(1) \quad A\mathbf{y} + \mathbf{b} \leqslant 0, \qquad \mathbf{y} \geqslant 0,$$

minimisant la forme linéaire ${}^t\mathbf{c}\mathbf{y}$.

S*. *Chercher la solution du système*

$$(2) \quad {}^tA\mathbf{z} + \mathbf{c} \geqslant 0, \qquad \mathbf{z} \geqslant 0,$$

maximisant la forme linéaire ${}^t\mathbf{b}\mathbf{z}$.

Problème canonique de minimisation

C. *Chercher la solution du système*

$$(\mathrm{I}) \quad \begin{aligned} &\alpha_{i1}y_1 + \ldots + \alpha_{in}y_n + \beta_i = 0 \qquad (i = 1, \ldots, m), \\ &y_1 \geqslant 0, \ldots, y_n \geqslant 0, \end{aligned}$$

minimisant la forme linéaire $\gamma_1 y_1 + \ldots + \gamma_n y_n$.

Problème dual du problème C

C*. *Chercher la solution du système*

$$(\mathrm{II}) \quad \alpha_{1k}z_1 + \ldots + \alpha_{mk}z_m + \gamma_k \geqslant 0 \qquad (k = i, \ldots, n),$$

maximisant la forme linéaire $\beta_1 z_1 + \ldots + \beta_m z_m$.

Les conditions (I) et (II) sont appelées *contraintes linéaires des problèmes* C et C* respectivement. Les problèmes C et C* sont dits *duals l'un de l'autre.*

Sous forme matricielle ces problèmes s'énoncent de la façon suivante:

C. *Chercher la solution du système*

(I) $A\mathbf{y} + \mathbf{b} = 0, \qquad \mathbf{y} \geqslant 0,$

minimisant la forme linéaire ${}^t\mathbf{c}\mathbf{y}$.

C*. *Chercher la solution de l'inégalité*

(II) ${}^tA\mathbf{z} + \mathbf{c} \geqslant 0,$

maximisant la forme linéaire ${}^t\mathbf{b}\mathbf{z}$.

Vecteurs possibles et optimaux. Un problème de programmation linéaire est dit *possible* s'il existe un vecteur satisfaisant aux contraintes linéaires du problème. Si un tel vecteur existe il est dit *vecteur possible du problème.*

Un vecteur possible est dit *solution du problème* ou *vecteur optimal du problème* s'il minimise (dans les problèmes S et C) ou maximise (dans les problèmes S* et C*) la forme linéaire du problème. La valeur de ce minimum et de ce maximum est appelée *valeur du problème de programmation linéaire.*

Désignons par $x_1, \ldots, x_n$ les premiers membres des inégalités du système (II), autrement dit, posons

(3) $x_k = \alpha_{1k}z_1 + \ldots + \alpha_{mk}z_m + \gamma_k \qquad (k = 1, \ldots, n).$

Proposition 2.1. *Si le vecteur* $\begin{bmatrix} y_1 \\ \cdot \\ \cdot \\ \cdot \\ y_n \end{bmatrix}$ *vérifie les inégalités*

(1′) $\alpha_{i1}y_1 + \ldots + \alpha_{in}y_n + \beta_i \leqslant 0 \qquad (i = 1, \ldots, m),$

alors

$$x_1y_1 + \ldots + x_ny_n \leqslant {}^t\mathbf{c}\mathbf{y} - {}^t\mathbf{b}\mathbf{z}.$$

Démonstration. En raison de (3),

$$\begin{aligned} x_1y_1 + \ldots + x_ny_n &= (\alpha_{11}z_1 + \ldots + \alpha_{m1}z_m + \gamma_1)\, y_1 + \ldots \\ &\ldots + (\alpha_{1n}z_1 + \ldots + \alpha_{mn}z_m + \gamma_n)\, y_n = \\ &= (\alpha_{11}y_1 + \ldots + \alpha_{1n}y_n)\, z_1 + \ldots + (\alpha_{m1}y_1 + \ldots \\ &\ldots + \alpha_{mn}y_n)z_m + {}^t\mathbf{c}\mathbf{y}. \end{aligned}$$

De là, en vertu de (1′),

$$\begin{aligned} x_1y_1 + \ldots + x_ny_n &\leqslant -(\beta_1z_1 + \ldots + \beta_mz_m) + \\ &+ {}^t\mathbf{c}\mathbf{y} = {}^t\mathbf{c}\mathbf{y} - {}^t\mathbf{b}\mathbf{z}. \quad \square \end{aligned}$$

Corollaire 2.2. *Si* $\mathbf{y}$ *est un vecteur possible du problème standard de minimum et* $\mathbf{z}$ *un vecteur possible du problème dual, alors*

$$0 \leqslant x_1y_1 + \ldots + x_ny_n \leqslant {}^t\mathbf{c}\mathbf{y} - {}^t\mathbf{b}\mathbf{z}.$$

PROPOSITION 2.3. *Si le vecteur* $\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ *vérifie le système d'équations*

$$(\mathrm{I}') \qquad \alpha_{i1}y_1 + \ldots + \alpha_{in}y_n + \beta_i = 0 \qquad (i = 1, \ldots, m),$$

alors

$$x_1y_1 + \ldots + x_ny_n = {}^t\mathbf{c}\mathbf{y} - {}^t\mathbf{b}\mathbf{z}.$$

Cette proposition se démontre de façon analogue à la proposition (2.1).

COROLLAIRE 2.4. *Si* **y** *est un vecteur possible du problème canonique de minimum et* **z** *un vecteur possible du problème dual, alors*

$$0 \leqslant x_1y_1 + \ldots + x_ny_n = {}^t\mathbf{c}\mathbf{y} - {}^t\mathbf{b}\mathbf{z}.$$

PROPOSITION 2.5. *Si* **y** *est un vecteur possible du problème de minimum* (S *ou* C) *et* **z** *un vecteur possible du problème dual* (S* *ou* C*), *alors* ${}^t\mathbf{c}\mathbf{y} - {}^t\mathbf{b}\mathbf{z} \geqslant 0$.

La proposition 2.5 découle directement des corollaires 2.2 et 2.4.

PROPOSITION 2.6 (CRITÈRE D'OPTIMALITÉ DES VECTEURS). *Si* **y** *est un vecteur possible du problème de minimum,* **z** *un vecteur possible du problème dual et* ${}^t\mathbf{c}\mathbf{y} = {}^t\mathbf{b}\mathbf{z}$, *alors* **y** *et* **z** *sont des vecteurs optimaux des problèmes correspondants.*

D é m o n s t r a t i o n. Soit **y**′ un vecteur possible du problème du minimum. Selon la proposition 2.5,

$${}^t\mathbf{c}\mathbf{y}' \geqslant {}^t\mathbf{b}\mathbf{z}.$$

En outre, par hypothèse, ${}^t\mathbf{b}\mathbf{z} = {}^t\mathbf{c}\mathbf{y}$, donc ${}^t\mathbf{c}\mathbf{y}' \geqslant {}^t\mathbf{c}\mathbf{y}$ quel que soit le vecteur possible **y**′ du problème de minimum. Par conséquent, **y** est le vecteur optimal du problème de minimum.

De façon analogue on démontre que **z** est le vecteur optimal du problème de maximum. □

Théorème de dualité des problèmes standard. En théorie de programmation linéaire les théorèmes de dualité 2.7 et 2.8 sont essentiels.

THÉORÈME 2.7. *Si deux problèmes standard duals l'un de l'autre* (S *et* S*) *sont possibles, ces deux problèmes ont des solutions et les valeurs de ces problèmes sont identiques. Si au moins un des problèmes est impossible, alors aucun des problèmes n'a de solutions.*

D é m o n s t r a t i o n. Supposons que les deux problèmes sont possibles. Alors, le système

$$(1) \qquad A\mathbf{y} + \mathbf{b} \leqslant 0, \qquad \mathbf{y} \geqslant 0,$$

$$(2) \qquad {}^tA\mathbf{z} + \mathbf{c} \geqslant 0, \qquad \mathbf{z} \geqslant 0$$

est compatible.

La première partie du théorème sera démontrée si l'on démontre l'existence des solutions **y** et **z** respectivement pour les systèmes (1)

et (2) qui vérifient

(3) $\quad {}^t\mathbf{c}\mathbf{y} - {}^t\mathbf{b}\mathbf{z} \leqslant 0.$

En effet, dans ce cas, selon la proposition 2.5, les vecteurs possibles **y** et **z** vérifient l'inégalité ${}^t\mathbf{c}\mathbf{y} - {}^t\mathbf{b}\mathbf{z} \geqslant 0$. Donc, si **y** et **z** vérifient également (3), on a alors ${}^t\mathbf{c}\mathbf{y} = {}^t\mathbf{b}\mathbf{z}$. Par suite, en vertu du critère d'optimalité, les vecteurs **y** et **z** sont des vecteurs optimaux des problèmes correspondants (S et S*) et les valeurs des deux problèmes coïncideront. Il suffit ainsi de démontrer la compatibilité du système

$$(4) \quad \begin{cases} A\mathbf{y} + \mathbf{b} \leqslant 0, & \mathbf{y} \geqslant 0, \\ -{}^tA\mathbf{z} - \mathbf{c} \leqslant 0, & \mathbf{z} \geqslant 0, \\ {}^t\mathbf{c}\mathbf{y} - {}^t\mathbf{b}\mathbf{z} \leqslant 0. \end{cases}$$

Ecrivons ce système sous forme matricielle:

$$(4) \quad \begin{bmatrix} A & 0 \\ 0 & -{}^tA \\ {}^t\mathbf{c} & -{}^t\mathbf{b} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{y} \\ \mathbf{z} \end{bmatrix} + \begin{bmatrix} \mathbf{b} \\ -\mathbf{c} \\ 0 \end{bmatrix} \leqslant 0, \qquad \begin{bmatrix} \mathbf{y} \\ \mathbf{z} \end{bmatrix} \geqslant 0.$$

Selon le théorème 2.6, le système (4) est compatible si et seulement si est incompatible le système

$$(5) \quad \begin{bmatrix} {}^tA & 0 & \mathbf{c} \\ 0 & -A & -\mathbf{b} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{u} \\ \mathbf{v} \\ \lambda \end{bmatrix} \geqslant 0, \qquad {}^t\mathbf{b}\mathbf{u} - {}^t\mathbf{c}\mathbf{v} > 0, \qquad \begin{bmatrix} \mathbf{u} \\ \mathbf{v} \\ \lambda \end{bmatrix} \geqslant 0.$$

Ce système peut être écrit sous forme

$$(5) \quad \begin{array}{llll} A\mathbf{v} + \mathbf{b}\lambda \leqslant 0, & & & \\ -{}^tA\mathbf{u} - \mathbf{c}\lambda \leqslant 0, & \mathbf{u} \geqslant 0, & \mathbf{v} \geqslant 0, & \lambda \geqslant 0, \\ {}^t\mathbf{c}\mathbf{v} - {}^t\mathbf{b}\mathbf{u} < 0. & & & \end{array}$$

Montrons que le système (5) est incompatible. Admettons qu'il existe des vecteurs **u** et **v** et un nombre réel λ vérifiant les inégalités (5). Alors pour $\lambda > 0$ on a:

$$(5') \quad \begin{array}{ll} A(\mathbf{v}\lambda^{-1}) + \mathbf{b} \leqslant 0, & \mathbf{v}\lambda^{-1} \geqslant 0, \\ -{}^tA(\mathbf{u}\lambda^{-1}) - \mathbf{c} \leqslant 0, & \mathbf{u}\lambda^{-1} \geqslant 0, \\ {}^t\mathbf{c}(\mathbf{v}\lambda^{-1}) - {}^t\mathbf{b}(\mathbf{u}\lambda^{-1}) < 0. & \end{array}$$

Les premières quatre inégalités montrent que les vecteurs $\mathbf{v}\lambda^{-1}$ et $\mathbf{u}\lambda^{-1}$ satisfont respectivement aux conditions (1) et (2), c'est-à-dire sont des vecteurs possibles des problèmes correspondants. Par consé-

quent, selon la proposition 2.5,

$$ {}^t\mathbf{c}\,(\mathbf{v}\lambda^{-1}) - {}^t\mathbf{b}\,(\mathbf{u}\lambda^{-1}) \geqslant 0, $$

ce qui contredit la dernière inégalité (5′).

Mais si $\lambda = 0$, le système (5) est incompatible. En effet, par hypothèse, est compatible le système (1), (2), c'est-à-dire le système

$$ (6) \quad \begin{bmatrix} A & 0 \\ 0 & -{}^tA \end{bmatrix} \begin{bmatrix} \mathbf{y} \\ \mathbf{z} \end{bmatrix} + \begin{bmatrix} \mathbf{b} \\ -\mathbf{c} \end{bmatrix} \leqslant \mathbf{0}, \qquad \begin{bmatrix} \mathbf{y} \\ \mathbf{z} \end{bmatrix} \geqslant \mathbf{0}. $$

Selon le théorème 2.6, de la compatibilité du système (6) s'ensuit l'incompatibilité du système

$$ \begin{bmatrix} {}^tA & 0 \\ 0 & -A \end{bmatrix} \begin{bmatrix} \mathbf{u} \\ \mathbf{v} \end{bmatrix} \geqslant \mathbf{0}, \qquad {}^t\mathbf{b}\mathbf{u} - {}^t\mathbf{c}\mathbf{v} > 0, \qquad \begin{bmatrix} \mathbf{u} \\ \mathbf{v} \end{bmatrix} \geqslant \mathbf{0}, $$

c'est-à-dire est incompatible le système

$$ \begin{aligned} &A\mathbf{v} \leqslant \mathbf{0}, \\ &-{}^tA\mathbf{u} \leqslant \mathbf{0}, \qquad \mathbf{u} \geqslant 0, \qquad \mathbf{v} \geqslant 0, \\ &{}^t\mathbf{c}\mathbf{v} - {}^t\mathbf{b}\mathbf{u} < 0. \end{aligned} $$

Ainsi, le système (5) est incompatible et, par suite, le système (4) est compatible.

Supposons maintenant qu'est possible seul l'un des deux problèmes duals l'un de l'autre, par exemple, le problème S, tandis que S* ne l'est pas. Démontrons qu'alors le problème S n'a pas de solutions. La possibilité du premier problème signifie qu'il existe une solution $\mathbf{y}'$ du système (1), c'est-à-dire

$$ (1') \quad A\mathbf{y}' + \mathbf{b} \leqslant \mathbf{0}, \qquad \mathbf{y}' \geqslant \mathbf{0}. $$

L'impossibilité du problème S*, c'est-à-dire l'incompatibilité du système

$$ (2) \quad -{}^tA\mathbf{z} - \mathbf{c} \leqslant \mathbf{0}, \qquad \mathbf{z} \geqslant \mathbf{0}, $$

implique, selon le théorème 1.12, la compatibilité du système

$$ (2^*) \quad A\mathbf{x} \leqslant \mathbf{0}, \qquad {}^t\mathbf{c}\mathbf{x} \leqslant 0, \qquad \mathbf{x} \geqslant \mathbf{0}. $$

Par conséquent, il existe un vecteur $\mathbf{x}'$ tel que

$$ (2') \quad A\mathbf{x}' \leqslant \mathbf{0}, \qquad {}^t\mathbf{c}\mathbf{x}' < 0, \qquad \mathbf{x}' \geqslant \mathbf{0}. $$

Sur la base de (1′) et (2′) on conclut que pour tout n naturel se vérifient les inégalités

$$ (7) \quad A\,(\mathbf{y}' + n\mathbf{x}') + \mathbf{b} \leqslant \mathbf{0}, \qquad \mathbf{y}' + n\mathbf{x}' \geqslant \mathbf{0}. $$

Donc, pour tout n naturel le vecteur $\mathbf{y}' + n\mathbf{x}'$ est un vecteur possible du premier problème. Toutefois, la forme linéaire ${}^t\mathbf{c}\mathbf{y}$ n'a pas de

minimum. En effet,

$$ {}^t\mathbf{c}(\mathbf{y}' + n\mathbf{x}') = {}^t\mathbf{c}\mathbf{y}' + n({}^t\mathbf{c}\mathbf{x}') $$

et dans la somme du second membre le premier terme est un certain nombre réel, tandis que le second terme, en raison de ${}^t\mathbf{c}\mathbf{x}' < 0$, peut être rendu, pour un n suffisamment grand, inférieur à tout nombre donné. Donc, la forme linéaire ${}^t\mathbf{c}\mathbf{y}$ n'a pas de minimum, autrement dit, le premier problème n'a pas de solutions. □

Théorème de dualité pour problèmes canoniques. Examinons les problèmes canoniques C et C*:

C. *Chercher la solution du système* $A\mathbf{y} + \mathbf{b} = 0$, $\mathbf{y} \geqslant 0$, *minimisant la forme linéaire* ${}^t\mathbf{c}\mathbf{y}$.

C*. *Chercher la solution de l'inégalité* ${}^tA\mathbf{z} + \mathbf{c} \geqslant 0$, *maximisant la forme linéaire* ${}^t\mathbf{b}\mathbf{z}$.

Le problème C est équipotent au problème standard suivant:

S_1. *Chercher la solution du système*

$$ \begin{bmatrix} -A \\ A \end{bmatrix} \mathbf{y} + \begin{bmatrix} -\mathbf{b} \\ \mathbf{b} \end{bmatrix} \leqslant 0, \qquad \mathbf{y} \geqslant 0, $$

minimisant la forme linéaire ${}^t\mathbf{c}\mathbf{y}$.

Le problème dual de S_1 est le problème suivant:

S_1^*. *Chercher la solution du système*

$$ [-{}^tA \mid {}^tA] \begin{bmatrix} \mathbf{z}' \\ \mathbf{z}'' \end{bmatrix} + \mathbf{c} \geqslant 0, \qquad \begin{bmatrix} \mathbf{z}' \\ \mathbf{z}'' \end{bmatrix} \geqslant 0, $$

où $\mathbf{z}' = \begin{bmatrix} z_1 \\ \cdot \\ \cdot \\ \cdot \\ z_m \end{bmatrix}$, $\mathbf{z}'' = \begin{bmatrix} z_{m+1} \\ \cdot \\ \cdot \\ \cdot \\ z_{2m} \end{bmatrix}$, *qui maximise la forme linéaire*

$$ [-{}^t\mathbf{b} \mid {}^t\mathbf{b}] \begin{bmatrix} \mathbf{z}' \\ \mathbf{z}'' \end{bmatrix}. $$

On voit sans peine que le problème S_1^* est équipotent au problème C*. En effet,

$$ [-{}^tA \mid {}^tA] \begin{bmatrix} \mathbf{z}' \\ \mathbf{z}'' \end{bmatrix} = {}^tA(\mathbf{z}'' - \mathbf{z}'), \qquad [-{}^t\mathbf{b} \mid {}^t\mathbf{b}] \begin{bmatrix} \mathbf{z}' \\ \mathbf{z}'' \end{bmatrix} = {}^t\mathbf{b}(\mathbf{z}'' - \mathbf{z}'). $$

Tout vecteur de dimension m peut être représenté sous forme d'une différence de deux vecteurs non négatifs de dimension m. Par suite, si l'on pose $\mathbf{z} = \mathbf{z}'' - \mathbf{z}'$, $\mathbf{z}$ parcourt l'ensemble de tous les vecteurs de dimension m de $\mathbf{R}^m$ quand $\mathbf{z}''$ et $\mathbf{z}'$ parcourent l'ensemble de tous les vecteurs non négatifs de $\mathbf{R}^m$.

Par conséquent, le problème S_1^* est équivalent au problème suivant (coïncidant avec le problème C*). *Chercher la solution de l'inégalité* ${}^tA\mathbf{z} + \mathbf{c} \geqslant 0$, *maximisant la forme linéaire* ${}^t\mathbf{b}\mathbf{z}$.

20—01762

Les problèmes standard S_1 et S_1^* sont duals l'un de l'autre et pour eux se vérifie le théorème de dualité. Les problèmes C et C* sont respectivement équipotents aux problèmes S_1 et S_1^*. Donc, le théorème de dualité s'applique aussi aux problèmes C et C*, c'est-à-dire qu'on a le théorème suivant.

THÉORÈME 2.8. *Si deux problèmes canoniques duals l'un de l'autre* (C *et* C*) *sont possibles, alors les deux problèmes admettent des solutions et les valeurs de ces problèmes coïncident. Si l'un au moins de ces problèmes est impossible, alors aucun des problèmes n'admet de solutions.*

Théorème d'équilibre. Rappelons qu'on a convenu de désigner par $x_1, \ldots, x_n$ les premiers membres des inégalités du système (II),

$$x_k = \alpha_{1k}z_1 + \ldots + \alpha_{mn}z_m \qquad (k = 1, \ldots, n).$$

THÉORÈME 2.9. *Soient* $\mathbf{y} = \begin{bmatrix} y_1 \\ \cdot \\ \cdot \\ \cdot \\ y_n \end{bmatrix}$ *le vecteur possible du problème canonique de minimum et* $\mathbf{z} = \begin{bmatrix} z_1 \\ \cdot \\ \cdot \\ \cdot \\ z_m \end{bmatrix}$ *le vecteur possible du problème dual. Si*

$$(*) \qquad x_1y_1 = 0, \ldots, x_ny_n = 0,$$

alors $\mathbf{y}$ *et* $\mathbf{z}$ *sont des vecteurs optimaux des problèmes correspondants* (C *et* C*).

D é m o n s t r a t i o n. Supposons que les conditions (*) sont satisfaites. Selon le corollaire 2.4, on a

$$(1) \qquad 0 \leqslant x_1y_1 + \ldots + x_ny_n = {}^t\mathbf{c}\mathbf{y} - {}^t\mathbf{b}\mathbf{z}.$$

Sur la base de (*) et (1) on conclut que ${}^t\mathbf{c}\mathbf{y} - {}^t\mathbf{b}\mathbf{z} = 0$. Selon le critère d'optimalité les vecteurs $\mathbf{y}$ et $\mathbf{z}$ sont des vecteurs optimaux respectivement des problèmes C et C*. □

R e m a r q u e. La condition (*) est également nécessaire pour que les vecteurs possibles $\mathbf{y}$ et $\mathbf{z}$ soient optimaux. En effet, selon le corollaire 2.4, (1) est vérifié. Si les vecteurs $\mathbf{y}$ et $\mathbf{z}$ sont optimaux, alors, selon le théorème 2.8,

$$(2) \qquad {}^t\mathbf{c}\mathbf{y} = {}^t\mathbf{b}\mathbf{z}.$$

De (1) et (2) il s'ensuit

$$0 \leqslant x_1y_1 + \ldots + x_ny_n = 0.$$

Puisque $\mathbf{y}$ et $\mathbf{z}$ sont des vecteurs possibles, on a $x_1, \ldots, x_n \geqslant 0$ et $y_1, \ldots, y_n \geqslant 0$. De là s'ensuivent les égalités (*).

Exercices

1. Montrer que si l'un des problèmes duals l'un de l'autre de la programmation linéaire (canoniques ou standard) admet une solution, alors l'autre problème a également une solution.
2. Donner un exemple de problème standard (canonique) de minimum à deux variables qui, ainsi que son dual, ne soit pas possible.
3. Construire un exemple de problème standard de minimum admettant plus d'une solution optimale.

§ 3. Méthode du simplexe (méthode de Dantzig)

Méthode du simplexe. La méthode du simplexe a été mise au point par Dantzig pour des problèmes de programmation linéaire. Dans la méthode simple de résolution simultanée de deux problèmes canoniques duals l'un de l'autre exposée plus loin on se réfère à Hall [28].

Considérons les problèmes canoniques duals l'un de l'autre.

C. *Chercher la solution du système*

$$\text{(I)}\qquad \begin{array}{l} \alpha_{11}y_1+\ldots+\alpha_{1n}y_n+\beta_1=0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ \alpha_{m1}y_1+\ldots+\alpha_{mn}y_n+\beta_m=0, \end{array}\qquad y_1\geqslant 0,\ \ldots,\ y_n\geqslant 0,$$

minimisant la forme linéaire v:

$$\gamma_1y_1+\ldots+\gamma_ny_n=v.$$

C*. *Chercher la solution du système*

$$\text{(II)}\qquad \begin{array}{l} \alpha_{11}z_1+\ldots+\alpha_{m1}z_m+\gamma_1\geqslant 0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ \alpha_{1n}z_1+\ldots+\alpha_{mn}z_m+\gamma_n\geqslant 0, \end{array}$$

maximisant la forme linéaire u:

$$\beta_1z_1+\ldots+\beta_mz_m=u.$$

La méthode du simplexe est la méthode permettant de résoudre simultanément les problèmes canoniques C et C* duals l'un de l'autre.

Soit $A=\begin{bmatrix}\alpha_{11} & \ldots & \alpha_{1n}\\ \ldots & \ldots & \ldots\\ \alpha_{m1} & \ldots & \alpha_{mn}\end{bmatrix}$ la matrice du système d'équations (I).

On admettra plus loin que le rang de la matrice A est m; cette hypothèse simplifie quelque peu l'exposé schématique de la méthode du simplexe. On peut réduire le cas général à ce cas étudié.

Considérons le tableau

$$
\begin{array}{c|ccccccc|l}
 & & & \eta & & \eta^* & & & \\
\hline
 & & & \vdots & & \vdots & & & \\
x^* & \cdots & & \alpha & \cdots & \beta & & \cdots & = -y^* \\
 & & & \vdots & & \vdots & & & \\
x & \cdots & & \gamma & \cdots & \delta & & \cdots & = -y \\
 & & & \vdots & & \vdots & & & \\
\hline
 & & & = z^* & & = z & & &
\end{array}
$$

Ce tableau se prête à la représentation simultanée de deux systèmes d'équations linéaires. Il représente le système linéaire suivant les lignes :

$$
(1) \qquad
\begin{array}{l}
\vdots \\
\ldots + \alpha\eta^* + \ldots + \beta\eta + \ldots = -y^*, \\
\vdots \\
\ldots + \gamma\eta^* + \ldots + \delta\eta + \ldots = -y \\
\vdots
\end{array}
$$

et suivant les colonnes :

$$
(2) \qquad
\begin{array}{l}
\vdots \\
\ldots + \alpha x^* + \ldots + \gamma x + \ldots = z^*, \\
\vdots \\
\ldots + \beta x^* + \ldots + \delta x + \ldots = z. \\
\vdots
\end{array}
$$

La *transformation du tableau avec élément pivot* α ($\alpha \neq 0$) substitue au tableau de départ le tableau correspondant à la solution du système (1) par rapport à $-\eta^*$ et à la solution du système (2) par rapport à x^*.

Une fois résolue l'équation du système (1) comportant l'élément pivot α par rapport à $-\eta^*$, il vient

$$\ldots + \alpha^{-1}y^* + \ldots + \alpha^{-1}\beta\eta + \ldots = -\eta^*.$$

En portant cette expression de $-\eta^*$ dans les autres équations du système (1), on obtient:

$$(1)\qquad \begin{array}{l} \ldots + \alpha^{-1} y^* + \ldots + \alpha^{-1}\beta\eta + \ldots = -\eta^*, \\ \ldots - \alpha^{-1}\gamma y^* + \ldots + (\delta - \alpha^{-1}\beta\gamma)\,\eta + \ldots = -y. \end{array}$$

De façon analogue, en résolvant le système (2) par rapport à x^*, il vient

$$(2)\qquad \begin{array}{l} \vdots \qquad\qquad\qquad \vdots \\ \ldots + \alpha^{-1} z^* + \ldots + (-\alpha^{-1}\gamma)\, x + \ldots = x^*, \\ \vdots \qquad\qquad\qquad \vdots \\ \ldots + \alpha^{-1}\beta z^* + \ldots + (\delta - \alpha^{-1}\beta\gamma)\, x + \ldots = z. \\ \vdots \qquad\qquad\qquad \vdots \end{array}$$

Ainsi, la transformation du tableau avec élément pivot α remplace le tableau de départ par le tableau suivant:

		y^*		η		
z^*	$\cdots$	α^{-1}	$\cdots$	$\alpha^{-1}\beta$	$\cdots$	$=-\eta^*$
$\vdots$		$\vdots$				
x	$\cdots$	$-\alpha^{-1}\gamma$	$\cdots$	$\delta-\alpha^{-1}\beta\gamma$	$\cdots$	$=-y$
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	
	$\cdots$	$=x^*$	$\cdots$	$=z$		

correspondant à la solution du système (1) suivant les lignes par rapport à $-\eta^*$ et du système (2) suivant les colonnes par rapport à x^*.

Les deux problèmes canoniques C et C* duals l'un de l'autre trouvent leur représentation dans le tableau

		y_1	$\cdots$	y_n	1	
	z_1	α_{11}	$\cdots$	α_{1n}	β_1	$=0$
T_1	$\cdot\cdot$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdot\ \cdot$
	z_m	α_{m1}	$\cdots$	α_{mn}	β_m	$=0$
	1	γ_1	$\cdots$	γ_m	0	$=v$
		$=x_1$	$\cdots$	$=x_n$	$=u$	

Cherchons simultanément la solution des deux problèmes. Chassons d'abord les variables $z_1, \ldots, z_m$ non soumises aux contraintes. C'est la première étape de la résolution. Elle est mise en œuvre par une succession de transformations avec pivot en partant du tableau T_1.

Les opérations s'effectuent jusqu'à l'apparition dans le tableau d'un élément non nul avec y au-dessus et zéro à droite sur la ligne. On obtient finalement le tableau de la forme

		$y'_{m+1} \cdots y'_n$	$0 \cdots 0$	1	
T'_1	x'_1				$= -y'_1$
	$\vdots$				$\vdots$
	x'_m				$= -y'_m$
	1	$\gamma'_{m+1} \cdots \gamma'_n$			$= v$
		$= x'_{m+1} \quad = x'_n$	$= z'_1 \cdots = z'_m$	$= u$	

$$(x'_i \geqslant 0, \quad y'_j \geqslant 0)$$

Dans ce tableau les variables avec primes représentent en un arrangement différent les variables figurant dans le tableau de départ T_1, les lignes et les colonnes ayant été permutées par rapport à la position des zéros. Les m dernières colonnes représentent les équations exprimant les variables $z'_1, \ldots, z'_m$ en fonction des variables $x'_1, \ldots, x'_m$. Ces équations doivent être extraites:

$$\text{(III)} \quad \begin{aligned} z'_1 &= d_{11}x'_1 + \ldots + d_{1m}x'_m, \\ &\ldots\ldots\ldots\ldots\ldots \\ z'_m &= d_{m1}x'_1 + \ldots + d_{mm}x'_m. \end{aligned}$$

Ensuite, il ne faut considérer que les égalités liant les variables x'_i et y'_j, qui sont exprimées par la partie du tableau T'_1 comportant les $n - m$ premières colonnes. Ainsi, après élimination des variables $z_1, \ldots, z_m$, on aboutit au tableau

		$y_{m+1} \cdots y_n$	1	
T	x_1		β_1	$= -y_1$
	$\vdots$		$\vdots$	
	x_m		β_m	$= -y_m$
	1	$c_{m+1} \cdots c_n$	d	$= v$
		$x_{m+1} \cdots x_n$	u	

Le tableau T est dit *possible suivant les lignes* si sont remplies les conditions

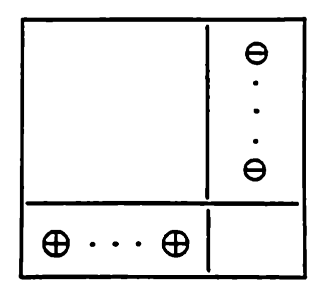
(1) $\beta_1 \leqslant 0, \ \ldots, \ \beta_m \leqslant 0.$

Ces conditions traduisent que le vecteur $(-\beta_1, \ldots, -\beta_m, 0, \ldots, 0)$ est le vecteur possible du problème C, c'est-à-dire qu'il vérifie le système (I). Supposons que le tableau T est possible suivant les lignes, c'est-à-dire que les conditions (1) sont satisfaites. L'objectif de l'étape suivante de résolution du problème est de rechercher par une série de transformations avec pivot dans le tableau obtenu à partir de T les vecteurs possibles des deux problèmes (C et C*) satisfaisant aux conditions

$$(*) \quad x_1y_1 = 0, \ \ldots, \ x_ny_n = 0 \qquad (x_i \geqslant 0, \quad y_j \geqslant 0).$$

Selon le théorème d'équilibre, ces vecteurs seront des vecteurs optimaux des problèmes correspondants.

Introduisons les notations: $\oplus$ un nombre non négatif, $\ominus$ un nombre non positif. Posons qu'on part du tableau T et que l'on est en mesure de passer au tableau de la forme



Alors, en dotant les variables libres $x_1, \ldots, x_m$ et $y_{m+1}, \ldots, y_n$ de valeurs nulles, on obtient les vecteurs possibles des deux problèmes (C et C*) constituant des vecteurs optimaux de ces problèmes.

Voyons l'influence de la transformation avec élément pivot α_{rs} sur la colonne des termes libres et la valeur de la forme linéaire v à minimiser:

$$\begin{array}{lll} \alpha_{rs} \ldots \beta_r & \ldots \ \alpha_{rs}^{-1} & \ldots \ \alpha_{rs}^{-1}\beta_r, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \alpha_{ts} \ldots \beta_t & \ldots -\alpha_{rs}^{-1}\alpha_{ts} & \ldots \ \beta_t - \alpha_{rs}^{-1}\beta_r\alpha_{ts}, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \gamma_s \ \ldots \ \delta & \ldots -\alpha_{rs}^{-1}\gamma_s & \ldots \ \delta - \alpha_{rs}^{-1}\beta_r\gamma_s. \end{array}$$

On suppose que dans le tableau (à gauche) les éléments β_t de la colonne des termes libres ne sont pas positifs, c'est-à-dire

$$(1) \quad \beta_t \leqslant 0 \qquad (i = 1, \ldots, m).$$

Il nous faut que la nouvelle valeur de la forme linéaire v ne soit pas supérieure à la précédente, c'est-à-dire que $\delta - \alpha_{rs}^{-1}\beta_r\gamma_s \leqslant \delta$. Cette inégalité se vérifie si sont satisfaites les conditions

$$(\alpha) \quad \alpha_{rs} > 0, \qquad \gamma_s < 0.$$

Avec la satisfaction de ces conditions la nouvelle valeur de la forme linéaire v n'est pas supérieure à la précédente, en outre, la nouvelle valeur de la forme v pour $\beta_r < 0$ est strictement inférieure à la précédente.

De plus, il nous faut que les nouveaux éléments de la colonne des termes libres soient non positifs, c'est-à-dire que

$$\beta_i - \alpha_{rs}^{-1}\beta_r\alpha_{is} \leqslant 0.$$

Avec la satisfaction des conditions (α) et pour $\alpha_{is} \leqslant 0$ cette inégalité est vérifiée. Si, par contre, $\alpha_{is} > 0$ l'inégalité peut s'écrire sous forme

$$(\beta) \quad \frac{\beta_r}{\alpha_{rs}} \geqslant \frac{\beta_i}{\alpha_{is}} \quad \text{pour tous} \quad \alpha_{is} > 0 \quad (i \neq r).$$

On aboutit ainsi à la *règle* suivante *de sélection de l'élément pivot* de la transformation du tableau possible suivant les lignes.

Soit un tableau possible suivant les lignes. *En guise d'élément pivot (de la transformation) il nous faut choisir l'élément α_{rs} si sont satisfaites les conditions*:

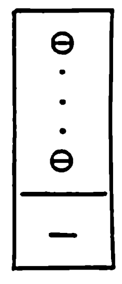
$$(\alpha) \quad \gamma_s < 0, \quad \alpha_{rs} > 0;$$

$$(\beta) \quad \frac{\beta_r}{\alpha_{rs}} \geqslant \frac{\beta_i}{\alpha_{is}} \quad \text{avec} \quad \alpha_{is} > 0 \quad (i \neq r).$$

Le choix de l'élément pivot conformément à cette règle garantit la possibilité d'un nouveau tableau suivant les lignes et pour $\beta_r < 0$ fournit une nouvelle valeur de la forme linéaire v (à minimiser) strictement inférieure à la précédente.

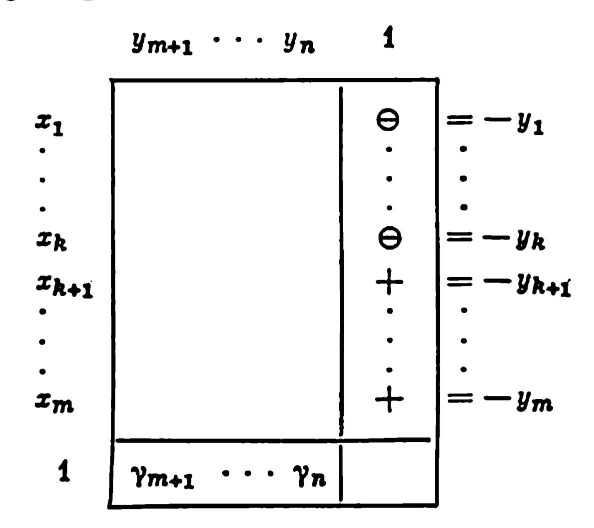
En partant du tableau possible on effectue par lignes la succession des transformations avec pivot en se conformant à la règle de choix de l'élément pivot. L'opération s'achève quand dans la dernière ligne du tableau il n'y a plus d'éléments négatifs; cela signifie que le tableau est possible aussi bien par lignes que par colonnes, c'est-à-dire qu'on a trouvé les solutions des deux problèmes C et C* (on a obtenu les vecteurs optimaux).

Le processus prend aussi fin au cas où on se heurte dans le tableau à une colonne négative (qui n'est pas la dernière) de la forme



et, par suite, la règle de choix de l'élément pivot est inapplicable. Cela signifie que le problème C* est impossible, car on ne peut satisfaire à la condition $x_s \geqslant 0$.

Le tableau T peut s'avérer impossible aussi bien par lignes que par colonnes. Dans ce cas en cherchant la solution possible du problème C ou en établissant l'impossibilité du problème C* on agit de la façon suivante. Les lignes du tableau T sont permutées de façon que toutes les lignes possibles soient en haut du tableau:

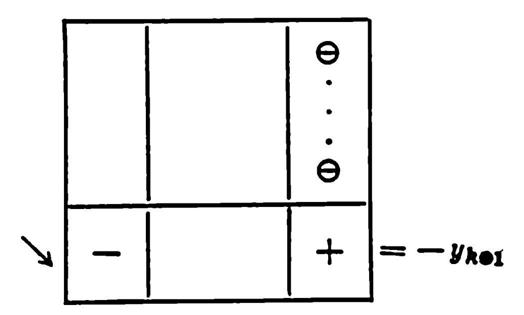


Les $k+1$ premières lignes de ce tableau seront considérées comme un tableau possible par lignes et on tâchera de minimiser $(-y_{k+1})$. Si au cours du cheminement on aboutit à une valeur non positive de $(-y_{k+1})$, on obtiendra alors $k+1$ lignes possibles ou davantage. On poursuit le processus de façon analogue en recherchant la représentation du plus grand nombre de lignes en forme possible. Si une ligne positive apparaît dans le tableau, c'est-à-dire une ligne (impossible) de la forme

$\oplus \cdots \oplus$	$+$

cela signifiera que le problème C est impossible, car on ne peut satisfaire à la condition $-y_j \leqslant 0$.

Si, par contre, il s'avère que la valeur minimale de $(-y_{k+1})$ est positive, on a le tableau de la forme



Dans ce cas en guise d'élément pivot on choisit l'élément marqué par une flèche. On vérifie sans peine que ce choix fournit $k+1$

lignes possibles ou davantage. On a ainsi obtenu le procédé permettant de trouver la solution possible du problème C dans tous les cas réalisables.

P r o b l è m e. Chercher la solution du système

$$\text{(I)}\quad \begin{aligned} &5y_1 - 4y_2 + 13y_3 - 2y_4 + y_5 - 20 = 0,\\ &y_1 - y_2 + 5y_3 - y_4 + y_5 - 8 = 0,\\ &y_1 \geqslant 0,\quad y_2 \geqslant 0,\quad y_3 \geqslant 0,\quad y_4 \geqslant 0,\quad y_5 \geqslant 0,\end{aligned}$$

minimisant la forme linéaire v,

$$y_1 + 6y_2 - 7y_3 + y_4 + 5y_5 = v.$$

Le problème dual à celui qu'on a donné peut être formulé ainsi : chercher la solution du système

$$\text{(II)}\quad \begin{aligned} &x_1 = 5z_1 + z_2 + 1 \geqslant 0,\\ &x_2 = -4z_1 - z_2 + 6 \geqslant 0,\\ &x_3 = 13z_1 + 5z_2 - 7 \geqslant 0,\\ &x_4 = -2z_1 - z_2 + 1 \geqslant 0,\\ &x_5 = z_1 + z_2 + 5 \geqslant 0,\end{aligned}$$

maximisant la forme linéaire u,

$$-20z_1 - 8z_2 = u.$$

Ces deux problèmes se représentent par le tableau suivant :

	y_1	y_2	y_3	y_4	y_5	1	
z_1	5	−4	13	−2	1	−20	$=0$
z_2	1	−1	5	−1	**1**	−8	$=0$
1	1	6	−7	1	5	0	$=v$
	x_1	x_2	x_3	x_4	x_5	$=u$	

Cherchons simultanément les solutions des deux problèmes. Chassons d'abord les inconnues z_1 et z_2. En chassant z_2 par transformation avec élément pivot 1 (noté en caractère gras) il vient

	y_1	y_2	y_3	y_4	0	1	
z_1	4	−3	8	−1	−1	−12	$=0$
x_5	1	−1	5	−1	1	−8	$=-y_5$
1	−4	11	−32	6	−5	40	$=v$
	x_1	x_2	x_3	x_4	z_2	$=u$	

A présent chassons z_2 par transformation avec élément pivot 4 de la première colonne:

	0	y_2	y_3	y_4	0	1	
x_1	1/4	−3/4	2	−1/4	−1/4	−3	$=-y_1$
x_5	−1/4	−1/4	3	−3/4	5/4	−5	$=-y_5$
1	1	8	−24	5	−6	28	$=v$
	z_1	x_2	x_3	x_4	z_2	$=u$	

La première et la cinquième colonnes montrent que z_1 et z_2 s'expriment en fonction de x_1 et x_5 de la façon suivante:

$$\text{(III)}\qquad \begin{aligned} z_1 &= \frac{1}{4}x_1 - \frac{1}{4}x_5 + 1\,; \\ z_2 &= -\frac{1}{4}x_1 + \frac{5}{4}x_5 - 6. \end{aligned}$$

En éliminant la première et la cinquième colonnes dans le tableau précédent, il vient

	y_2	y_3	y_4	1	
x_1	−3/4	2	−1/4	−3	$=-y_1$
x_5	−1/4	3	−3/4	−5	$=-y_5$
1	8	−24	5	28	$=v$
	x_2	x_3	x_4	$=u$	

Ce tableau est possible par lignes. En accord avec la règle de choix de l'élément pivot on adopte 2 dans la seconde colonne et en réalisant la transformation on aboutit au tableau

	y_2	y_1	y_4	1	
x_3	−3/8	1/2	−1/8	−3/2	$=-y_3$
x_5	7/8	−3/2	−3/8	−1/2	$=-y_5$
1	−1	12	2	−8	$=v$
	x_2	x_1	x_4	$=u$	

Dans le tableau obtenu on choisit l'élément 7/8 dans la première colonne en guise d'élément pivot et, en réalisant la transformation

on aboutit au tableau

	y_5	y_1	y_4	1	
x_3	3/7	—1/7	—2/7	—12/7	$= -y_3$
x_2	8/7	—12/7	—3/7	—4/7	$= -y_2$
1	8/7	72/7	11/7	—60/7	$= v$
	x_5	x_1	x_4	$= u$	

Ce tableau est possible aussi bien par lignes que par colonnes. En supposant les variables « libres » x_2, x_3, y_1, y_4, y_5 égales à zéro, il vient :

$$x_1 = 72/7,\ x_2 = 0,\ x_3 = 0,\ x_4 = 11/7,\ x_5 = 8/7,$$

$$y_1 = 0,\ y_2 = 4/7,\ y_3 = 12/7,\ y_4 = 0,\ y_5 = 0.$$

En portant les valeurs trouvées de x_1 et x_5 dans les formules (III), on obtient $z_1 = 23/7$, $z_2 = -50/7$. Par conséquent, le vecteur (0, 4/7, 12/7, 0, 0) est la solution du premier problème, tandis que le vecteur (23/7, —50/7) est la solution du problème dual. De plus, $u = v = -60/7$, c'est-à-dire que la valeur minimale de la forme linéaire v et la valeur maximale de la forme linéaire u sont égales (—60/7).

Exercices

1. Maximiser la forme linéaire $2x_1 + 3x_2$ en remplissant les conditions $4x_1 + 2x_2 + x_3 = 4$ et $x_1 + 3x_2 = 5$.

2. Maximiser la forme linéaire $x_1 + 3x_2 + x_3$ en remplissant les conditions

$$5x_1 + 3x_2 \leqslant 3, \qquad x_1 + 2x_2 + 4x_3 \leqslant 4.$$

3. Résoudre le problème de la compatibilité du système d'inéquations linéaires

$$5x_1 + 4x_2 - 7x_3 \leqslant 1,$$

$$-x_1 + 2x_2 - x_3 \leqslant -4,$$

$$-3x_1 - 2x_2 + 4x_3 \leqslant 3,$$

$$3x_1 - 2x_2 - 2x_3 \leqslant -7.$$

4. Etablir si le système d'inégalités linéaires suivant est compatible :

$$4x_1 - 5x_2 \geqslant 3,$$

$$-2x_1 - 7x_2 \geqslant 1,$$

$$-2x_1 + x_2 \geqslant -2.$$

5. Est-ce que le système d'équations linéaires

$$3x_1 - 5x_2 + 2x_3 = 0,$$
$$2x_1 - 4x_2 + x_3 = 0$$

admet des solutions non négatives non nulles?

6. Démontrer que le système d'inéquations linéaires

$$5x_1 - 4x_2 \leqslant 7,$$
$$-3x_1 + 3x_2 \leqslant -5$$

n'a pas de solutions non négatives.

7. Chercher les solutions non négatives du système d'équations linéaires:

$$5x_1 + x_2 + 6x_3 - 5x_5 = 2;$$
$$-7x_1 - x_2 - 2x_3 + x_4 + 2x_5 = -5.$$

CHAPITRE X

GROUPES

§ 1. Semi-groupes et monoïdes

Semi-groupes. Soit A un ensemble non vide. L'opération binaire $*$ sur l'ensemble A est dite *associative* si $a * (b * c) = (a * b) * c$ pour tous éléments a, b, c de A. L'opération binaire $*$ est dite *commutative* si pour tous a, b de A, on a $a * b = b * a$.

C'est ainsi que les opérations d'addition et de multiplication d'entiers sont associatives et commutatives. L'opération de soustraction d'entiers est ni associative ni commutative.

DÉFINITION. On appelle *semi-groupe* l'algèbre $\langle A, *\rangle$ du type (2) à opération binaire associative $*$. Une sous-algèbre d'un semi-groupe est appelée *sous-semi-groupe*.

Exemples. 1. Soit $+$ une opération d'addition sur l'ensemble **N** des nombres naturels. L'algèbre $\langle \mathbf{N}, +\rangle$ est un semi-groupe, vu que l'opération d'addition est associative. Ce semi-groupe est dit *semi-groupe additif des nombres naturels.*

2. Soit M un ensemble non vide et A la collection de toutes les applications de l'ensemble M dans lui-même avec la loi de composition d'applications $\circ$ en guise d'opération binaire. L'algèbre $\langle A, \circ\rangle$ est un semi-groupe, vu que la composition d'applications est associative. Ce semi-groupe est appelé *semi-groupe d'applications de l'ensemble M dans lui-même.*

Monoïdes. Soit A un ensemble à opération binaire $*$. L'élément e de A est dit *élément neutre par rapport à l'opération* $*$ si $a * e = e * a = a$ pour tout a de A.

DÉFINITION. On appelle *monoïde* l'algèbre $\langle A, *, e\rangle$ du type (2, 0), dont les opérations principales satisfont aux conditions:

(1) l'opération binaire $*$ est associative;

(2) l'élément e est un élément neutre par rapport à l'opération $*$.

Exemples. 1. Soit $+$ une opération d'addition sur l'ensemble **N** des nombres naturels. L'algèbre $\langle \mathbf{N}, +, 0\rangle$ est un monoïde, vu que l'addition est associative et 0 est un élément neutre par rapport à l'addition. Ce monoïde est appelé *monoïde additif des nombres naturels.*

2. Soit $\cdot$ l'opération de multiplication sur l'ensemble **N** des nombres naturels. L'algèbre $\langle \mathbf{N}, \cdot, 1\rangle$ est un monoïde, vu que la multi-

plication est associative et 1 est un élément neutre par rapport à la multiplication. Ce monoïde s'appelle *monoïde multiplicatif des nombres naturels.*

3. Soient n un nombre naturel fixé différent de zéro, A la collection de toutes les applications de l'ensemble $\{1, \ldots, n\}$ dans lui-même et ε une application identique de cet ensemble. L'algèbre $\langle A, \circ, \varepsilon\rangle$, où $\circ$ est une opération binaire (composition d'applications), est un monoïde, vu que la composition d'applications est associative et ε est un élément neutre par rapport à l'opération $\circ$. Ce monoïde s'appelle *monoïde d'applications de l'ensemble* $\{1, \ldots, n\}$ *dans lui-même.*

4. Soit $\mathcal{K} = \langle K, +, -, \cdot, 1\rangle$ un anneau. L'algèbre $\langle K, \cdot, 1\rangle$ est alors un monoïde. Il s'appelle *monoïde multiplicatif de l'anneau* $\mathcal{K}$.

Loi associative généralisée. Soient A un ensemble non vide et $*$ une opération binaire sur ce dernier. Soit $a_1, a_2, \ldots, a_n$ une suite de n éléments de A. Désignons par le symbole

$$a_1 * a_2 * \ldots * a_n$$

la *composition de la suite d'éléments* définie de façon inductive ainsi:

$$a_1 * \ldots * a_{n-1} * a_n = (a_1 * \ldots * a_{n-1}) * a_n.$$

Selon cette définition,

$$a * b * c = (a * b) * c; \qquad a * b * c * d = (a * b * c) * d.$$

Si la loi de composition est une multiplication, la composition d'éléments $a_1, \ldots, a_n$ est alors appelée *produit* et est habituellement notée $\prod_{i=1}^{n} a_i$; au cas d'une notation additive de la composition d'éléments $a_1, \ldots, a_n$ elle porte le nom de *somme* et est habituellement notée $\sum_{i=1}^{n} a_i$.

Si l'opération binaire $*$ sur l'ensemble A est associative, on montre sans peine que

$$\begin{aligned} a * b * c * d &= (a * b) * (c * d) = \\ &= a * (b * c) * d = \\ &= (a * b * c) * d = \\ &= a * (b * c * d). \end{aligned}$$

Au cas d'une opération binaire associative sur A, l'étude d'une composition quelconque d'une suite d'éléments de A, peut être menée en plaçant les parenthèses de façon quelconque, comme le montre le théorème suivant.

THÉORÈME 1.1. *Soient A un ensemble à opération binaire associative* $*$ *et* $a_1, \ldots, a_n$ *une suite d'éléments de A. Soient* $1 < n_1 < n_2 < \ldots < n_k \leqslant n$, *où* $n_1, \ldots, n_k$ *sont des nombres naturels, et*

$$b_0 = a_1 * \ldots * a_{n_1-1}, \ b_1 = a_{n_1} * \ldots * a_{n_2-1}, \ldots \\ \ldots, b_k = a_{n_k} * \ldots * a_n,$$

alors $a_1 * \ldots * a_n = b_0 * \ldots * b_k$.

Démonstration (s'effectue par récurrence sur n). Si $n = 2$, le théorème est apparemment vrai. Supposons que le théorème est vrai si la suite comprend $n - 1$ éléments au plus.

Premier cas : $n_k = n$. Dans ce cas $b_k = a_n$. Par définition,

$$a_1 * \ldots a_n = (a_1 * \ldots a_{n-1}) * a_n.$$

Par hypothèse de récurrence,

$$a_1 * \ldots * a_{n-1} = b_0 * \ldots * b_{k-1};$$

par conséquent,

$$a_1 * \ldots * a_n = (b_0 * \ldots * b_{k-1}) * b_k = b_0 * \ldots * b_k.$$

Deuxième cas: $n_k < n$. Dans ce cas

$$b_k = (a_{n_k} * \ldots * a_{n-1}) * a_n = b'_k * a_n,$$

où $b'_k = a_{n_k} * \ldots * a_{n-1}$, et

$$a_1 * \ldots * a_{n-1} = b_0 * \ldots * b'_k$$

(selon l'hypothèse de récurrence) ; par conséquent,

$$\begin{aligned} a_1 * \ldots * a_n &= (a_1 * \ldots * a_{n-1}) * a_n = \\ &= (b_0 * \ldots * b'_k) * a_n = \text{(par hypothèse de récurrence)} \\ &= ((b_0 * \ldots * b_{k-1}) * b'_k) * a_n = \\ &= (b_0 * \ldots * b_{k-1}) * (b'_k * a_n) = \\ &= (b_0 * \ldots * b_{k-1}) * b_k = \\ &= b_0 * \ldots * b_k. \ \square \end{aligned}$$

Considérons le cas particulier où l'opération associative binaire sur l'ensemble A est une multiplication et $a_1 = a_2 = \ldots = a_n = a$, où $a \in A$. Alors, par définition,

$$a^n = a_1 \cdot a_2 \ldots a_n = \prod_{i=1}^{n} a_i.$$

COROLLAIRE 1.2. *Soient A un ensemble avec une opération binaire associative de multiplication donnée sur A et* $a \in A$. *Alors, pour tous*

nombres naturels m et n différents de zéro, on a:

$$a^{m+n} = a^m a^n, \qquad a^{mn} = (a^m)^n.$$

Considérons également le cas où l'opération binaire associative sur l'ensemble A est une addition et $a_1 = a_2 = \ldots = a_n = a$, où $a \in A$. Alors, par définition,

$$na = a_1 + \ldots + a_n = \sum_{i=1}^{n} a_i.$$

COROLLAIRE 1.3. *Soient A un ensemble avec opération binaire associative d'addition donnée sur A et $a \in A$. Alors,*

$$(m + n)\, a = ma + na, \qquad (mn)\, a = m\, (na)$$

pour tous nombres naturels n et m différents de zéro.

Exercices

1. Soit $\langle A, \cdot, 1\rangle$ un monoïde multiplicatif. Démontrer que pour tout élément a du monoïde et m et n naturels quelconques, on a les relations

$$a^m a^n = a^{m+n}, \qquad (a^m)^n = a^{mn}.$$

2. Soient $\langle A, +, 0\rangle$ un monoïde additif et $a \in A$. Montrer que pour tous m et n naturels, on a

$$ma + na = (m + n)\, a, \qquad n\, (ma) = (nm)\, a.$$

3. Soit $\langle \mathrm{N}, +\rangle$ un semi-groupe additif des nombres naturels. Chercher le système des générateurs de ce semi-groupe.

4. Soit $\langle \mathrm{N}, +, 0\rangle$ un monoïde additif des nombres naturels. Décrire tous les sous-monoïdes de ce monoïde.

5. Soit $\langle \mathrm{N}^*, \cdot\rangle$ un semi-groupe multiplicatif des nombres naturels différents de zéro. Chercher le système minimal des générateurs de ce semi-groupe.

6. Soit $\langle \mathrm{N}, \cdot\rangle$ un semi-groupe multiplicatif des nombres naturels. Chercher le système des générateurs du semi-groupe contenu dans tout autre système des générateurs de ce semi-groupe.

§ 2. Sous-groupes et classes suivant un sous-groupe

Sous-groupes. Soient M un ensemble non vide et S_M un ensemble de toutes les permutations de l'ensemble M, c'est-à-dire la collection de toutes les applications injectives de l'ensemble M sur lui-même. Si f et g sont des permutations de l'ensemble M, leur composition $f \circ g$ et l'application inverse f^{-1} sont alors des permutations de l'ensemble M.

THÉORÈME 2.1. *L'algèbre $\langle S_M, \circ, {}^{-1}\rangle$ est un groupe.*

D é m o n s t r a t i o n. L'opération binaire $\circ$ sur S_M, composition de permutations de l'ensemble M, est associative en vertu du théorème 2.2. La permutation identique i_M est un élément neutre

par rapport à l'opération $\circ$. Pour toute permutation f de l'ensemble M, $f \circ f^{-1} = i_M$. Donc, l'algèbre $\langle S_M, \circ, {}^{-1} \rangle$ est un groupe. □

DÉFINITION. Le groupe $\langle S_M, \circ, {}^{-1} \rangle$ est dit *groupe symétrique* sur l'ensemble M et noté $\mathcal{S}_M$. Si l'ensemble M est fini et comprend n éléments, le groupe $\mathcal{S}_M$ est alors dit *groupe symétrique de degré n* et noté $\mathcal{S}_n$.

Soit $\mathcal{G} = \langle G, \cdot, {}^{-1} \rangle$ un groupe multiplicatif. A chaque élément a du groupe associons l'application t_a de l'ensemble G sur G définie par la formule

$$t_a (x) = ax \text{ pour tout } x \text{ de } G.$$

L'application t_a est une permutation de l'ensemble G et est appelée *translation à gauche de G*. L'ensemble $T(G) = \{t_a \mid a \in G\}$ est appelé *ensemble des translations à gauche de G*.

PROPOSITION 2.2. *Soit $\mathcal{S}_G = \langle S_G, \circ, {}^{-1} \rangle$ un groupe symétrique sur l'ensemble G. L'algèbre $\mathcal{T} = \langle T(G), \circ, {}^{-1} \rangle$ est un sous-groupe du groupe $\mathcal{S}_G$.*

D é m o n s t r a t i o n. Pour tous éléments a, b du groupe $\mathcal{G}$ on a les égalités

$$(1) \quad t_a \circ t_b = t_{ab} \quad \text{et} \quad t_a \circ t_a^{-1} = i_G = t_e,$$

où e est l'unité du groupe $\mathcal{G}$. En effet, pour tout x de G

$$(t_a \circ t_b)(x) = t_a (t_b (x)) = t_a (bx) = abx = t_{ab} (x), \quad \text{c'est-à-dire} \quad t_a \circ t_b = t_{ab}.$$

En posant dans la dernière égalité $b = a^{-1}$, il vient $t_a \circ t_a^{-1} = t_e = i_G$, où e est l'unité du groupe $\mathcal{G}$.

En outre, en vertu de (1), $t_a \circ t_e = t_{ae} = t_a$ et

$$(2) \quad (t_a)^{-1} = t_a^{-1} \in T(G).$$

Sur la base de (1) et (2) on conclut que l ensemble $T(G)$ est fermé relativement aux opérations principales du groupe $S(G)$. Par conséquent, l'algèbre $\langle T(G), \circ, {}^{-1} \rangle$ est un sous-groupe du groupe S_G. □

THÉORÈME 2.3. (DE CAYLEY). *Tout groupe $\mathcal{G} = \langle G, \circ, {}^{-1} \rangle$ est isomorphe au sous-groupe du groupe symétrique sur l'ensemble G. En particulier, chaque groupe fini d'ordre n est isomorphe au sous-groupe du groupe symétrique de degré n.*

D é m o n s t r a t i o n. Soit $T(G)$ la collection de toutes les translations à gauche de l'ensemble G. Selon le théorème 2.2, le groupe $\mathcal{T} = \langle T(G), \circ, {}^{-1} \rangle$ est un sous-groupe du groupe S_G.

Soit h une application de l'ensemble G sur $T(G)$ définie par la formule

$$h(a) = t_a \text{ pour tout } a \text{ de } G.$$

L'application h respecte les opérations principales du groupe $\mathcal{G}$.

En effet, en vertu de (1) et (2), on a

$$h(ab) = t_{ab} = t_a \circ t_b = h(a) \circ h(b),$$

$$h(a^{-1}) = t_{a^{-1}} = (t_a)^{-1} = (h(a))^{-1}.$$

De plus, h est une application injective. En effet, pour tous a, b de l'ensemble G si $h(a) = h(b)$, on a $t_a = t_b$, $t_a(l) = t_b(e)$, où e est l'unité du groupe $\mathscr{G}$, $ae = be$, et, par suite, $a = b$. Donc, h est un isomorphisme du groupe $\mathscr{G}$ sur le sous-groupe $\mathscr{T}$ du groupe symétrique S_G sur l'ensemble G. □

Classes suivant un sous-groupe. Soit $\mathscr{H} = \langle H, \cdot, ^{-1}\rangle$ un sous-groupe du groupe $\mathscr{G} = \langle G, \cdot, ^{-1}\rangle$. Introduisons sur l'ensemble G la relation binaire $\equiv$:

$a \equiv b \pmod H$ si et seulement si $ab^{-1} \in H$; appelons cette relation *congruence suivant le sous-groupe* $\mathscr{H}$.

PROPOSITION 2.4. *Soit $\mathscr{H}$ un sous-groupe du groupe $\mathscr{G}$. La congruence sur G suivant le sous-groupe $\mathscr{H}$ est une relation d'équivalence.*

Démonstration. Vu que $aa^{-1} \in H$, on a $a \equiv a \pmod H$, c'est-à-dire que la congruence suivant $\mathscr{H}$ est réflexive. Puisque de $ab^{-1} \in H$ s'ensuit $ba^{-1} \in H$, de $a \equiv b \pmod H$ s'ensuit $b \equiv \equiv a \pmod H$: la congruence suivant $\mathscr{H}$ est symétrique. Ensuite, pour tous éléments a, b, c de G si $ab^{-1} \in H$ et $bc^{-1} \in H$, alors $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$. Donc, si $a \equiv b$ et $b \equiv c \pmod H$, alors $a \equiv c \pmod H$: la congruence suivant H est transitive. Ainsi, la congruence suivant $\mathscr{H}$ est une relation d'équivalence. □

Exemple. Soient $\langle V, +, -\rangle$ un groupe additif de l'espace vectoriel $\mathscr{V}$, $\mathscr{L}$ un sous-espace de l'espace $\mathscr{V}$ et $\langle L, +, -\rangle$ son groupe additif. Considérons sur V la relation binaire $\sim$:

$a \sim b$ si et seulement si $a - b \in L$, appelée *congruence des vecteurs de V en sens de $\mathscr{L}$*. Cette relation est une relation d'équivalence sur V. Les classes d'équivalence s'appellent variétés linéaires de l'espace $\mathscr{V}$ de sens $\mathscr{L}$.

DÉFINITION. Les classes d'équivalence de la congruence suivant le sous-groupe $\mathscr{H}$ s'appellent *classes à droite du groupe $\mathscr{G}$* suivant le sous-groupe $\mathscr{H}$.

Notons les principales propriétés des classes suivant un sous-groupe.

PROPRIÉTÉ 2.1. *Toutes deux classes à droite du groupe $\mathscr{G}$ suivant le sous-groupe $\mathscr{H}$ soit coïncident soit sont disjointes. L'ensemble G est la réunion de toutes les classes à droite du groupe $\mathscr{G}$ suivant le sous-groupe $\mathscr{H}$.*

Cette propriété découle directement du théorème 2.4.1.

Soit $g \in G$. Notons Hg l'ensemble défini par l'égalité $Hg = \{hg \mid h \in H\}$.

PROPRIÉTÉ 2.2. *Si $g \in G$, alors Hg est une classe à droite du groupe $\mathscr{G}$ suivant le sous-groupe $\mathscr{H}$.*

D é m o n s t r a t i o n. Soit A la classe à droite du groupe $\mathcal{G}$ suivant le sous-groupe $\mathcal{H}$ comprenant g. Démontrons que $A = Hg$. Soit hg tout élément de Hg. Alors, $hgg^{-1} \in H$ et $hg \equiv g \pmod H$. Donc, $Hg \subset A$. Inversement : si $c \in A$, c'est-à-dire $c \equiv g \pmod H$, alors, $cg^{-1} = h \in H$ et $c = hg \in Hg$. Donc $A \subset Hg$. Par conséquent, $A = Hg$. □

PROPRIETE 2.3. *Soient A la classe à droite du groupe $\mathcal{G}$ suivant le sous-groupe $\mathcal{H}$ et $g \in A$, alors $A = Hg$.*

D é m o n s t r a t i o n. Les classes A et Hg possèdent un élément commun g. Selon la propriété 2.1 elles coïncident, c'est-à-dire $A = Hg$. □

PROPRIETE 2.4. *Soit $\mathcal{H}$ un sous-groupe fini du groupe $\mathcal{G}$, $g \in G$. Alors, le nombre d'éléments de la classe Hg vaut le nombre d'éléments de l'ensemble H.*

D é m o n s t r a t i o n. Soit m le nombre d'éléments de l'ensemble H: $H = \{h_1, \ldots, h_m\}$. Alors $Hg = \{h_1g, \ldots, h_mg\}$ et $h_ig \neq h_kg$ pour $i \neq k$, car de $h_ig = h_kg$, selon la règle de simplification, s'ensuivrait l'égalité $h_i = h_k$. Par conséquent, le nombre d'éléments de l'ensemble Hg vaut m.

Soit $\mathcal{H}$ le sous-groupe du groupe $\mathcal{G}$. Introduisons sur l'ensemble G la relation binaire $\sim$ de la façon suivante :

$a \sim b \pmod H$ si et seulement si $b^{-1}a \in H$; appelons-la *congruence à gauche suivant le sous-groupe $\mathcal{H}$*. Une vérification directe montre que cette relation est une équivalence sur l'ensemble G. Les classes d'équivalence de cette relation s'appellent *classes à gauche du groupe $\mathcal{G}$* suivant le sous-groupe $\mathcal{H}$. On vérifie sans peine que les classes à gauche possèdent des propriétés analogues aux propriétés 2.1-2.4.

Théorème de Lagrange. Soit $\mathcal{G}$ un groupe fini. Le nombre d'éléments de son ensemble de base G est appelé *ordre du groupe $\mathcal{G}$*.

THEOREME 2.5 (de Lagrange). *L'ordre du sous-groupe d'un groupe fini est un diviseur de l'ordre du groupe.*

D é m o n s t r a t i o n. Soient $\mathcal{H}$ un sous-groupe du groupe fini $\mathcal{G}$ et

$H, Hg_2, \ldots, Hg_k$

l'ensemble de toutes les classes à droite variées du groupe $\mathcal{G}$ suivant le sous-groupe $\mathcal{H}$. Alors

(1) $G = H \cup Hg_2 \cup \ldots \cup Hg_k$,

en outre, deux classes quelconques inclues dans cette réunion sont disjointes. Aussi, si n est le nombre d'éléments de l'ensemble G et m le nombre d'éléments de l'ensemble H, a-t-on, selon la propriété 2.4, que le nombre d'éléments de toute classe Hg_i vaut m et, en vertu de (1), $n = mk$. □

COROLLAIRE 2.6. *Si $\mathcal{G}$ est un groupe fini d'ordre n et $g \in G$, alors, l'ordre de l'élément g divise n.*

COROLLAIRE 2.7. *Tout groupe fini d'ordre simple est cyclique.*

Exercices

1. Soient $\mathscr{S}_n = \langle S_n, \cdot, ^{-1}\rangle$ un groupe symétrique des permutations de degré n et A_n un ensemble de toutes les permutations paires de S_n. Montrer que $\mathscr{A}_n = \langle \overline{A}_n, \cdot, ^{-1}\rangle$ est un sous-groupe du groupe $\mathscr{S}_n$.

2. Montrer que pour un sous-groupe arbitraire d'un groupe multiplicatif les éléments inverses des éléments de la classe à gauche constituent des éléments de la classe à droite.

3. Démontrer que pour $n > 1$ les $n - 1$ transpositions (12), (13), ..., $(1n)$ engendrent le groupe symétrique $\mathscr{S}_n$.

4. Montrer que pour $n > 2$ les $n - 2$ cycles à trois termes (123), ..., $(12n)$ engendrent le groupe $\mathscr{A}_n$ des permutations paires.

5. Soit $\mathscr{G} = \langle G, \cdot, ^{-1}\rangle$ un groupe multiplicatif des matrices inversibles $n \times n$ sur le corps $\mathscr{F}$. Soit H un ensemble de toutes les matrices de G dont le déterminant vaut l'unité du corps $\mathscr{F}$. Montrer que $\langle H, \cdot, ^{-1}\rangle$ est un sous-groupe du groupe $\mathscr{G}$.

6. Soient $\mathbf{R}^*$ un ensemble de tous les nombres réels différents de zéro et $\mathscr{R}^* = \langle \mathbf{R}^*, \cdot, ^{-1}\rangle$ le groupe multiplicatif des nombres réels. Montrer que pour tout nombre naturel $n \geqslant 1$ le groupe multiplicatif des racines n-ièmes de l'unité est l'unique sous-groupe d'ordre n du groupe $\mathscr{R}^*$.

§ 3. Groupes cycliques

Ordre de l'élément du groupe. Soient $\mathscr{G} = \langle G, \cdot, ^{-1}\rangle$ un groupe multiplicatif, e son élément unité et $a \in G$.

DÉFINITION. On appelle *ordre de l'élément a du groupe* le plus petit nombre naturel m différent de zéro, tel que $a^m = e$. Si $a^n \neq e$ pour tout nombre naturel n non nul, a est alors appelé élément d'ordre infini.

L'ordre de l'élément a du groupe est noté $\mathcal{O}(a)$.

E x e m p l e. Dans un groupe multiplicatif des nombres complexes $\mathcal{O}(i) = 4$, $\mathcal{O}(-1) = 2$, $\mathcal{O}(1) = 1$, $\mathcal{O}(2) = \infty$.

On utilisera plus loin le théorème suivant (voir théorème 4.4.4 sur la division avec reste).

Pour des entiers n et $m > 0$ il existe des entiers q et r, tels que

$$(1) \quad n = m\cdot q + r, \quad 0 \leqslant r < m.$$

THÉORÈME 3.1. *Soit m un ordre (fini) de l'élément a d'un groupe multiplicatif. L'égalité $a^n = e$, où n est un entier, se vérifie si et seulement si m divise n.*

D é m o n s t r a t i o n. Posons que $a^n = e$ et démontrons que m divise n. Selon le théorème de la division avec reste, il existe pour des nombres n et m des entiers q et r satisfaisant aux conditions (1). Il s'agit de montrer que $r = 0$. En vertu de la condition $a^m = e$ et, par hypothèse, $a^n = e$. En vertu de (1), il s'ensuit que

$$a^n = a^{mq}\cdot a^r = (a^m)^q\cdot a^r = a^r = e.$$

Vu que $\mathcal{O}(a) = m$ et $0 \leqslant r < m$, il s'ensuit de $a^r = e$ que $r = 0$, c'est-à-dire que m divise n.

Supposons maintenant que m divise n et démontrons que $a^n = e$, m divisant n, on a $n = mk$ pour un certain entier k. Donc, $a^n = a^{mk} = (a^m)^k = e^k = e$, c'est-à-dire $a^n = e$. □

Proposition 3.2. *Soit a un élément du groupe multiplicatif muni d'un ordre fini m. L'égalité $a^r = a^s$, où r et s sont des entiers, se vérifie si et seulement si m divise r — s.*

Démonstration. L'égalité $a^r = a^s$ a lieu si et seulement si $a^{r-s} = e$. Selon le théorème 3.1, $a^{r-s} = e$ si et seulement si m divise $r - s$. Par conséquent, $a^r = a^s$ si et seulement si m divise $r - s$.

Corollaire 3.3. *Soit a un élément du groupe multiplicatif muni d'un ordre fini m. Soient r et s des entiers; $\bar{r} = r + m\mathbf{Z}$ et $\bar{s} = s + m\mathbf{Z}$ sont des classes résiduelles modulo m. L'égalité $a^r = a^s$ est vérifiée si et seulement si $\bar{r} = \bar{s}$.*

Corollaire 3.4. *Soit a un élément du groupe multiplicatif muni d'un ordre fini m. Les éléments e $(= a^0)$, a, a^2, . . ., a^{m-1} sont alors distincts.*

Proposition 3.5. *Soient a un élément du groupe multiplicatif d'ordre infini et r, s des entiers. L'égalité $a^r = a^s$ a lieu si et seulement si $r = s$.*

Démonstration. De l'égalité $r = s$ s'ensuit apparemment l'égalité $a^r = a^s$. Posons que $a^r = a^s$. Si $r \neq s$, par exemple, si $r > s$, alors $a^{r-s} = e$ et $r - s \neq 0$. C'est impossible, vu que, par hypothèse, l'élément a possède un ordre infini. Donc, $r = s$. □

Groupes cycliques. On donne plus loin la description des groupes cycliques.

Definition. Un groupe multiplicatif (additif) est dit *cyclique* si l'ensemble de base du groupe est composé de puissances (multiples) d'un élément quelconque du groupe; cet élément est appelé *élément générateur du groupe.*

Exemples. 1. Soit $\mathfrak{Z} = \langle \mathbf{Z}, +, - \rangle$ un groupe additif des entiers. Chaque élément du groupe est multiple de 1 (ou (—1)). Par conséquent, $\mathfrak{Z}$ est un groupe cyclique à élément générateur 1 (ou (—1)).

2. Le groupe de superpositions sur lui-même d'un polygone régulier de m angles est un groupe cyclique d'ordre m. Une rotation de $2\pi/m$ d'un polygone de m angles autour du centre est un élément générateur de ce groupe.

3. Soient m un entier positif, $\bar{k} = k + m\mathbf{Z}$ et $\mathbf{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ un ensemble de toutes les classes résiduelles modulo m. L'opération d'addition + et l'opération singulaire — se définissent ainsi:

$$\bar{k} + \bar{s} = \overline{k+s}, \quad -(\bar{k}) = (\overline{-k}) = (\overline{m-k}).$$

L'opération d'addition est associative et commutative. $\bar{0}$ est l'élément neutre par rapport à l'addition des classes et $\bar{k} + (\overline{-k}) = \bar{0}$. Par conséquent, l'algèbre $\mathfrak{Z}_m = \langle \mathbf{Z}_m, +, - \rangle$ est un groupe commutatif d'ordre m. C'est un groupe cyclique à élément générateur $\bar{1}$. Le groupe $\mathfrak{Z}_m$ est appelé *groupe additif des classes résiduelles modulo m.*

THÉORÈME 3.6. *Si l'élément générateur d'un groupe cyclique est muni d'un ordre infini, le groupe est alors isomorphe au groupe additif des entiers. Mais si l'élément générateur du groupe cyclique possède un ordre fini m, le groupe est alors isomorphe au groupe additif des classes résiduelles modulo m.*

Démonstration. Soit $\mathcal{G} = \langle G, \cdot, ^{-1} \rangle$ un groupe multiplicatif cyclique à élément générateur a, c'est-à-dire que $G = \{a^n \mid n \in \mathbf{Z}\}$. Soit $\mathfrak{Z} = \langle \mathbf{Z}, +, - \rangle$ un groupe additif des entiers et $\mathfrak{Z} = \langle \mathbf{Z}_m, +, - \rangle$ un groupe additif des classes résiduelles modulo m.

Premier cas: $\mathcal{O}(a) = \infty$. Dans ce cas, en vertu de la proposition 3.5, toutes les puissances entières de l'élément générateur a sont distinctes. Donc, l'application f de l'ensemble G sur $\mathbf{Z}$ telle que $f(a^n) = n$ pour tout n entier est injective. L'application f respecte les opérations principales du groupe $\mathcal{G}$ car pour tous entiers n et s:

$$f(a^n a^s) = f(a^{n+s}) = n + s = f(a^n) + f(a^s),$$
$$f(a^{-n}) = -n = -f(a^n).$$

Par conséquent, f est une application isomorphe du groupe $\mathcal{G}$ sur le groupe $\mathfrak{Z}$.

Second cas: $\mathcal{O}(a) = m$, l'élément a est muni d'un ordre fini m. Montrons que dans ce cas le groupe $\mathcal{G}$ est isomorphe au groupe $\mathfrak{Z}_m$. Démontrons que $G = \{e, a, a^2, \ldots, a^{m-1}\}$. Soit a^k un élément quelconque de G. Selon le théorème de division avec reste, il existe pour les nombres k et m des entiers q et r tels que

$$k = mq + r, \quad 0 \leqslant r < m.$$

Il s'ensuit que

$$a^k = a^{mq} a^r = a^r \in \{e, a, \ldots, a^{m-1}\};$$

par conséquent,

$$G = \{e, a, \ldots, a^{m-1}\}.$$

Considérons l'application φ de l'ensemble G sur l'ensemble $\mathbf{Z}_m$:

$$\mathbf{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\} \text{ telle que}$$
$$\varphi(a^k) = \bar{k} \text{ pour } k = 0, 1, \ldots, m-1.$$

En vertu de la proposition 3.2, φ est une application injective de l'ensemble G sur $\mathbf{Z}_m$. En outre, φ respecte les opérations principales

du groupe $\mathcal{G}$, de sorte que

$$\varphi(a^k a^s) = \varphi(a^{k+s}) = \overline{k+s} = \bar{k} + \bar{s} = \varphi(a^k) + \varphi(a^s),$$
$$\varphi(a^{-k}) = \overline{m-k} = -(\bar{k}).$$

Par conséquent, φ est une application isomorphe du groupe $\mathcal{G}$ sur le groupe $\mathfrak{Z}_m$. □

Sous-groupes du groupe cyclique. Montrons que tout sous-groupe du groupe cyclique est aussi cyclique.

THÉORÈME 3.7. *Tout sous-groupe du groupe cyclique est un groupe cyclique.*

Démonstration. Soit $\mathcal{G}$ un groupe multiplicatif cyclique à élément générateur a. Soit $\mathcal{H}$ le sous-groupe du groupe $\mathcal{G}$. Le théorème est apparemment vrai si H ne comprend qu'un seul élément. Supposons que H comprend plus d'un élément. Le sous-groupe $\mathcal{H}$ contient au moins une puissance positive de l'élément a car, autrement, si $a^{-k} \in H$, alors $(a^{-k})^{-1} = a^k \in H$. Soit a^s un élément de H avec un plus petit exposant positif de la puissance s. Tout élément de H est un élément de l'aspect a^k. Si $a^k \in H$, alors s divise k. En effet, selon le théorème de division avec reste (théorème 4.4.4) il existe pour les nombres k et s des entiers q et r tels que

(1) $\quad k = sq + r \quad$ et $\quad 0 \leqslant r < s.$

En raison de (1), $a^r = a^{k-sq} = a^k (a^s)^{-q} \in H$. Comme $a^r \in H$ et $0 \leqslant r < s$, en vertu du choix du nombre s, $r = 0$; donc $k = sq$. L'ensemble H est ainsi composé de puissances de l'élément a^s. Par conséquent, $\mathcal{H}$ est un groupe cyclique à élément générateur a^s. □

Exercices

1. Chercher tous les sous-groupes du groupe additif $\mathfrak{Z}$ de tous les entiers.
2. Chercher tous les sous-groupes du groupe cyclique d'ordre 12.
3. Chercher tous les sous-groupes du groupe cyclique d'ordre 24.
4. Démontrer qu'un groupe fini d'ordre simple est cyclique et que son élément quelconque, différent de l'élément neutre, est l'élément générateur.
5. Démontrer qu'il existe des groupes cycliques d'ordre arbitraire.
6. Démontrer que l'ordre d'un élément quelconque d'un groupe fini est un diviseur de l'ordre du groupe.
7. Soient m et n des nombres naturels premiers entre eux. Montrer que dans un groupe abélien multiplicatif le produit d'un élément a d'ordre m par un élément b d'ordre n est un élément d'ordre mn.
8. Montrer que tout groupe d'ordre 15 est cyclique.
9. Soit $\mathcal{G}$ un groupe multiplicatif des racines de 1 (racines de puissance n pour des nombres naturels quelconques $n > 0$). Montrer que pour tout nombre naturel m différent de zéro le groupe $\mathcal{G}$ ne possède qu'un seul sous-groupe d'ordre m et que chacun de ces sous-groupes est cyclique.

§ 4. Diviseurs normaux et groupes quotients

Diviseurs normaux du groupe. Soit $\mathcal{H}$ un sous-groupe du groupe $\mathcal{G}$. Une question se pose tout naturellement: à quelles conditions les partitions de l'ensemble G en classes à droite et à gauche suivant le sous-groupe $\mathcal{H}$ coïncident? Les sous-groupes munis de ces propriétés sont distingués au moyen de la définition suivante.

Définition. Un sous-groupe $\mathcal{H}$ du groupe $\mathcal{G}$ est appelé *diviseur normal du groupe* $\mathcal{G}$ si $g^{-1}hg \in H$ pour tout élément g de G et tout élément h de H.

La notation $\mathcal{H} \lhd \mathcal{G}$ signifie que $\mathcal{H}$ est un diviseur normal du groupe $\mathcal{G}$.

Exemples. 1. Soient $\mathcal{S}_n$ un groupe symétrique des permutations de degré n et $\mathcal{A}_n$ son sous-groupe de toutes les permutations paires. Alors $\mathcal{A}_n \lhd \mathcal{S}_n$.

2. Tout sous-groupe d'un groupe abélien est son diviseur normal.

3. Soient $\mathcal{G}$ un groupe multiplicatif des matrices inversibles $n \times n$ sur le corps $\mathcal{F}$ et $\mathcal{H}$ un sous-groupe des matrices dont les déterminants sont égaux à l'unité. Alors $\mathcal{H} \lhd \mathcal{G}$.

Voyons quelques propriétés des diviseurs normaux du groupe.

Propriété 4.1. *Le sous-groupe* $\mathcal{H}$ *du groupe* $\mathcal{G}$ *est un diviseur normal du groupe* $\mathcal{G}$ *si et seulement si chaque classe à droite du groupe* $\mathcal{G}$ *suivant le sous-groupe* $\mathcal{H}$ *est également une classe à gauche.*

Démonstration. Posons

(1) $\mathcal{H} \lhd \mathcal{G}$,

et démontrons que

(2) $Hg = gH$ pour tout g de G.

En vertu de (1), $g^{-1}hg \in H$ pour tout h de H. Aussi a-t-on $hg \in gH$ et $Hg \subset gH$. Ensuite, en vertu de (1), $(g^{-1})^{-1} hg^{-1} \in H$. Par conséquent, $gH \in Hg$ pour tout h de H, c'est-à-dire on est en présence d'une inclusion $gH \subset Hg$. Ainsi, de (1) découle (2).

Supposons maintenant qu'est satisfaite la condition (2). Alors, pour tout $h \in H$ il existe un $h_1 \in H$ tel que $hg = gh_1$. Par conséquent, $g^{-1}hg \in H$ pour tout $g \in G$ et tout $h \in H$, c'est-à-dire $\mathcal{H} \lhd \mathcal{G}$. Donc, de (2) s'ensuit (1). □

Propriété 4.2. *Soient* $\mathcal{A}$ *un sous-groupe du groupe* $\mathcal{B}$, $\mathcal{B}$ *étant un sous-groupe du groupe* $\mathcal{G}$ *et* $\mathcal{A} \lhd \mathcal{G}$; *alors* $\mathcal{A} \lhd \mathcal{B}$.

Démonstration. Soient a et b des éléments quelconques de $|\mathcal{A}|$ et $|\mathcal{B}|$ respectivement. Alors, $b^{-1}ab \in |\mathcal{A}|$, car, par hypothèse, $\mathcal{A} \lhd \mathcal{G}$. Donc, $\mathcal{A} \lhd \mathcal{B}$. □

Propriété 4.3. *Une intersection de toute collection de diviseurs normaux du groupe* $\mathcal{G}$ *est un diviseur normal du groupe* $\mathcal{G}$.

Démonstration. Soient $\mathcal{A} \lhd \mathcal{B}$ et $\mathcal{B} \lhd \mathcal{G}$. Alors $\mathcal{A} \cap \mathcal{B}$ est un sous-groupe du groupe $\mathcal{G}$. Si $c \in |\mathcal{A}| \cap |\mathcal{B}|$:

et $g \in G$, alors

$$g^{-1}cg \in |\mathcal{A}|, \qquad g^{-1}cg \in |\mathcal{B}|,$$

vu que $\mathcal{A}$ et $\mathcal{B}$, par hypothèse, sont des diviseurs normaux du groupe $\mathcal{G}$. Donc, $g^{-1}cg \in |\mathcal{A}| \cap |\mathcal{B}|$ et $\mathcal{A} \cap \mathcal{B} \lhd \mathcal{G}$.

De façon analogue, on démontre que la propriété 4.3 joue pour toute collection de diviseurs normaux du groupe $\mathcal{G}$. □

Groupe quotient. Soient $\mathcal{G} = \langle G, \cdot, ^{-1}\rangle$ un groupe multiplicatif et $A, B \subset G$. Définissons le produit $A \cdot B$ d'ensembles A et B par la formule

$$A \cdot B = \{x \cdot y \mid x \in A, y \in B\}.$$

PROPOSITION 4.1. *Soient $\mathcal{H}$ un diviseur normal du groupe $\mathcal{G}$ et G/H l'ensemble de toutes les classes du groupe $\mathcal{G}$ suivant le sous-groupe $\mathcal{H}$. Le produit de deux classes quelconques du groupe $\mathcal{G}$ suivant $\mathcal{H}$ est une classe suivant un sous-groupe. De plus,*

$$Ha \cdot Hb = Hab.$$

Démonstration. Soient ha et h_1b, où $h, h_1 \in H$, des éléments quelconques de Ha et Hb respectivement. Dans ce cas, $ah_1a^{-1} \in H$ puisque $\mathcal{H} \lhd \mathcal{G}$. Donc,

$$ha \cdot h_1b = h\,(ah_1a^{-1})\,ab \in Hab;$$

par conséquent, $(Ha)\cdot(Hb) \subset Hab$.

Démontrons l'inclusion inverse. Soit $hab \in Hab$. Alors $hab = (ha)\,b \in Ha \cdot Hb$. Donc $Hab \subset (Ha)\cdot(Hb)$; par conséquent, $(Ha)\cdot(Hb) = Hab$. □

Définissons sur l'ensemble G/H les opérations $\cdot$ et $^{-1}$ par les formules

$$(Ha)\cdot(Hb) = Hab, \qquad (Ha)^{-1} = Ha^{-1}$$

et considérons l'algèbre

$$\mathcal{G}/\mathcal{H} = \langle G/H, \cdot, ^{-1}\rangle.$$

THÉORÈME 4.2. *Soit $\mathcal{H}$ un diviseur normal du groupe $\mathcal{G} = \langle G, \cdot, ^{-1}\rangle$. L'algèbre $\mathcal{G}/\mathcal{H} = \langle G/H, \cdot, ^{-1}\rangle$ est un groupe.*

Démonstration. Soient $Ha, Hb \in G/H$. Les opérations dans G/H sont définies par les égalités

$$(1) \quad (Ha)\cdot(Hb) = Hab, \qquad (Ha)^{-1} = Ha^{-1}.$$

L'opération de multiplication des classes suivant un sous-groupe est associative. En effet, si $A = Ha$, $B = Hb$, $C = Hc$, alors, en vertu de (1),

$$A \cdot (B \cdot C) = (Ha)\cdot(Hbc) = Habc,$$

$$(A \cdot B)\cdot C = (Hab)\cdot(Hc) = Habc.$$

Donc, $A\,(BC) = (AB)\,C$ pour tous A, B, C de G/H.

L'élément H de G/H est un élément unité par rapport à la multiplication, car $A \cdot H = Ha \cdot He = Ha = A$, c'est-à-dire que $A \cdot H = A$ pour tout A de G/H. En vertu de (1), $A \cdot A^{-1} = Ha \cdot Ha^{-1} = Haa^{-1} = H$ pour tout élément A de G/H. Par conséquent, l'algèbre $\mathcal{G}/\mathcal{H}$ est un groupe. □

Définition. L'algèbre $\mathcal{G}/\mathcal{H}$ est dite *groupe quotient* du groupe $\mathcal{G}$ suivant le sous-groupe $\mathcal{H}$.

Exemples. 1. Soient $\mathfrak{Z}$ un groupe additif des entiers, m un nombre naturel fixé et $\bar{k} = k + m\mathbf{Z}$.

Alors,

$$\mathbf{Z}/m\mathbf{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\},$$

$$\bar{k} + \bar{n} = \overline{k+n}, \quad -(\bar{k}) = \overline{(-k)} = \overline{m-k}.$$

L'algèbre $\mathfrak{Z}/m\mathfrak{Z} = \langle \mathbf{Z}/m\mathbf{Z}, +, - \rangle$ est un groupe quotient du groupe $\mathfrak{Z}$ suivant le sous-groupe $m\mathfrak{Z}$.

2. Soient $\mathcal{S}_n$ un groupe symétrique des permutations de degré n $(n > 1)$ et $\mathcal{A}_n$ son sous-groupe des permutations paires. Alors, le groupe quotient $\mathcal{S}_n/\mathcal{A}_n$ est un groupe cyclique de deuxième ordre, vu que $S_n/A_n = \{A_n, A_n\sigma\}$, où σ est une certaine permutation impaire.

Noyau d'un homomorphisme. Soient $\mathcal{G} = \langle G, \cdot, {}^{-1}\rangle$ et $\mathcal{G}' = \langle G', \circ, {}^{-1}\rangle$ des groupes multiplicatifs.

Définition. Soit φ un homomorphisme du groupe $\mathcal{G}$ dans le groupe $\mathcal{G}'$. On appelle *noyau d'un homomorphisme* φ l'ensemble

$$\operatorname{Ker} \varphi = \{x \in G \mid \varphi(x) = e'\},$$

où e' est l'unité du groupe $\mathcal{G}'$.

L'ensemble $\operatorname{Ker} \varphi$ n'est pas vide, car $\varphi(e) = e'$. L'ensemble $\operatorname{Ker} \varphi$ est fermé dans le groupe $\mathcal{G}$ vu que pour tous a, b de $\operatorname{Ker} \varphi$ on a

$$\varphi(a \cdot b) = \varphi(a) \circ \varphi(b) = e' \circ e' = e';$$

$$\varphi(a^{-1}) = (\varphi(a))^{-1} = (e')^{-1} = e',$$

c'est-à-dire $a \cdot b$ et a^{-1} appartiennent à l'ensemble $\operatorname{Ker} \varphi$.

Définition. Un sous-groupe $\mathcal{G}$ avec ensemble de base $\operatorname{Ker} \varphi$, où φ est un homomorphisme du groupe $\mathcal{G}$, sera noté $\mathcal{K}er\, \varphi$:

$$\mathcal{K}er\, \varphi = \langle \operatorname{Ker} \varphi, \cdot, {}^{-1}\rangle$$

et on l'appellera *groupe du noyau d'un homomorphisme* φ ou simplement *noyau* φ.

Proposition 4.3. *Si φ est un homomorphisme du groupe $\mathcal{G}$ dans le groupe $\mathcal{G}'$, alors $\mathcal{K}er\, \varphi$ est un diviseur normal du groupe $\mathcal{G}$.*

Démonstration. On a montré plus haut que l'ensemble $\operatorname{Ker} \varphi$ est fermé relativement aux opérations principales du groupe

$\mathcal{G}$. En outre, pour tout g de G et tout h de Ker φ on a

$$\varphi(g^{-1}hg) = \varphi(g^{-1}) \circ e' \circ \varphi(g) = \varphi(g^{-1}eg) = \varphi(e) = e',$$

c'est-à-dire $g^{-1}hg \in$ Ker φ. Par conséquent, $\mathcal{K}er\ \varphi$ est un diviseur normal du groupe $\mathcal{G}$.

Proposition 4.4. *Soit φ un homomorphisme du groupe $\mathcal{G}$ dans le groupe $\mathcal{G}'$ avec noyau $\mathcal{H} = \langle H, \cdot, ^{-1}\rangle$. Pour tous a, b de G, si $\varphi(a) = \varphi(b)$, on a $Ha = Hb$.*

Démonstration. φ étant un homomorphisme et $\varphi(a) = \varphi(b)$, on a

$$\varphi(ab^{-1}) = \varphi(a) \circ \varphi(b^{-1}) = \varphi(a) \circ (\varphi(b))^{-1} = \varphi(a) \circ (\varphi(a))^{-1} = e'.$$

Par conséquent, $a \cdot b^{-1} \in H$ et $Ha = Hb$. □

Théorème des homomorphismes. Dans la théorie des groupes le théorème suivant sur les homomorphismes est un des principaux.

Théorème 4.5. *Soit f un homomorphisme du groupe $\mathcal{G}$ sur le groupe $\mathcal{G}'$ avec noyau $\mathcal{H}$. Le groupe quotient $\mathcal{G}/\mathcal{H}$ est alors isomorphe au groupe $\mathcal{G}'$.*

Démonstration. Soient $\mathcal{H} = \mathcal{K}er\ f$ et $H =$ Ker f. Soit $\bar{G} = G/H$ l'ensemble de toutes les classes du groupe $\mathcal{G}$ suivant le sous-groupe $\mathcal{H}$. Considérons l'application

$$\varphi \colon G/H \to G',$$

définie de la façon suivante:

(1) $\varphi(Ha) = f(a)$ pour toute classe suivant un sous-groupe Ha de $\bar{G}$.

Vu que Ker $f = H$, la valeur de $\varphi(Ha)$ ne dépend pas du choix du représentant de a dans la classe suivant un sous-groupe Ha. L'application φ respecte l'opération de multiplication dans le groupe $\mathcal{G}/\mathcal{H}$, car

$$\varphi(Ha \cdot Hb) = \varphi(Hab) = f(ab) = f(a) \cdot f(b) = \varphi(Ha)\,\varphi(Hb).$$

Donc, selon le théorème 3.3.1, φ est un homomorphisme du groupe $\mathcal{G}/\mathcal{H}$ dans le groupe $\mathcal{G}'$.

Par hypothèse, f est une application de G sur G'. En vertu de (1), il s'ensuit que φ est une application de G/H sur G'. L'application φ est injective. En effet, en vertu de (1), de l'égalité $\varphi(Ha) = \varphi(Hb)$ il s'ensuit que $f(a) = f(b)$; selon la proposition 4.4, il s'ensuit que $Ha = Hb$. Bref, on a établi que φ est une application injective de G/H sur G'. Par conséquent, φ est un homomorphisme du groupe quotient $\mathcal{G}/\mathcal{H}$ sur le groupe $\mathcal{G}'$. □

Exercices

1. Démontrer que tout groupe quotient d'un groupe additif $\mathfrak{X}$ des entiers est cyclique.

2. Chercher tous les groupes quotients d'un groupe cyclique d'ordre 12.

3. Démontrer que tout groupe quotient d'un groupe cyclique est cyclique.

4. Démontrer qu'un groupe quotient d'un groupe symétrique $\mathcal{S}_n$ de permutations de degré n suivant le sous-groupe $\mathcal{A}_n$ de toutes les permutations paires est un groupe cyclique de deuxième ordre.

5. Démontrer que le groupe additif $\mathfrak{X}$ des entiers est isomorphe au groupe additif $2\mathfrak{X}$ des nombres pairs.

6. Démontrer que le groupe additif de tous les nombres complexes est isomorphe au groupe additif de tous les vecteurs du plan.

7. Soit $\mathcal{G}$ un groupe des permutations. Considérons l'application h du groupe $\mathcal{G}$ dans le groupe multiplicatif des nombres $+1$ et -1 associant chaque permutation τ de $\mathcal{G}$ à sa signature sgn τ. Montrer que h est un homomorphisme.

8. Montrer que le groupe multiplicatif des racines m-ièmes de 1 est isomorphe au groupe additif $\mathfrak{X}_m$ des classes résiduelles modulo m.

9. Soient $\mathcal{G}$ le groupe multiplicatif des matrices inversibles et réelles $n \times n$ et $\mathcal{R}^*$ le groupe multiplicatif des nombres réels différents de zéro. Soit h l'application de $\mathcal{G}$ dans $\mathcal{R}^*$ associant chaque élément g du groupe $\mathcal{G}$ au déterminant $|g|$. Démontrer que h est un homomorphisme dont le noyau est le sous-groupe du groupe $\mathcal{G}$ de toutes les matrices $n \times n$ avec déterminants égaux à 1.

10. Soient $\mathcal{R}$ un groupe additif des nombres réels et $\mathcal{K}$ un groupe multiplicatif des nombres complexes dont le module vaut 1. Démontrer que l'application f de l'ensemble R dans K définie par la formule $f(x) = \cos 2\pi x + i \sin 2\pi x$ est un homomorphisme du groupe $\mathcal{R}$ sur le groupe $\mathcal{K}$ avec noyau Z.

11. Soient $\mathfrak{Q}$ un groupe additif des nombres rationnels et $\mathfrak{X}$ un groupe additif des entiers. Montrer que chaque élément du groupe quotient $\mathfrak{Q}/\mathfrak{X}$ possède un ordre fini. Démontrer que pour tout n naturel différent de zéro, $\mathfrak{Q}/\mathfrak{X}$ ne possède qu'un sous-groupe d'ordre n et que chacun de ces sous-groupes est cyclique.

CHAPITRE XI

THÉORIE DE DIVISIBILITÉ DANS L'ANNEAU DES ENTIERS

§ 1. Décomposition des entiers en facteurs premiers

Idéaux d'un anneau des entiers. Introduisons la notion d'idéal.

DEFINITION. Un ensemble non vide I des entiers est appelé *idéal d'un anneau* $\mathbb{Z}$ des entiers s'il est fermé par rapport à l'addition et à la multiplication sur tous entiers, c'est-à-dire si $a + b$, $ma \in \mathbf{Z}$ pour tous a, $b \in I$ et tout $m \in \mathbf{Z}$.

Il s'ensuit de la définition que tout idéal I est fermé par rapport à la soustraction et, partant, contient le nombre zéro.

Soit n un entier fixé quelconque. On vérifie sans peine que l'ensemble $n\mathbf{Z}$, $n\mathbf{Z} = \{nx \mid x \in \mathbf{Z}\}$, est un idéal de l'anneau $\mathbb{Z}$. Cet idéal est appelé *idéal principal* engendré par le nombre n. L'idéal $0 \cdot \mathbf{Z}$ n'est composé que d'un zéro et est appelé *idéal nul.* On voit aisément que $n\mathbf{Z} = (-n)\mathbf{Z}$. L'idéal engendré par le nombre n est également noté (n).

THÉORÈME 1.1. *Chaque idéal d'un anneau des entiers est principal. Si I est un idéal non nul de l'anneau $\mathbb{Z}$ et d le plus petit nombre positif contenu dans I, l'ensemble I est strictement composé de nombres multiples de d, c'est-à-dire $I = d\mathbf{Z}$.*

Démonstration. L'idéal nul est apparemment un idéal principal engendré par un zéro. Soit I un idéal non nul, c'est-à-dire comprenant au moins un nombre a différent de zéro. Alors, $a, -a \in I$ et l'un de ces nombres est positif. Soit d le plus petit nombre positif contenu dans I. L'idéal I comprend tous les multiples de d, c'est-à-dire $d\mathbf{Z} \subset I$. Il faut aussi montrer que tout nombre c de I est multiple de d. A cette fin, divisons c par d avec reste:

$$c = dq + r, \quad 0 \leqslant r < d, \quad q, r \in \mathbf{Z}.$$

Comme c et dq appartiennent à l'idéal I, on a $c - dq = r \in I$. Le cas de $r > 0$ est impossible, vu que d est le plus petit nombre positif contenu dans I. Par conséquent, $r = 0$ et $c = dq$. Ainsi, l'idéal I est strictement composé des multiples de d, $I = d\mathbf{Z}$. □

Nombres premiers. L'entier p est dit *premier* s'il est différent de zéro et de ± 1 et n'a pour diviseurs que ± 1 et $\pm p$. Un entier a différent de zéro et de ± 1 et possédant outre ± 1 et $\pm a$ d'autres diviseurs est appelé *nombre composé.*

Une vérification directe montre que les premiers facteurs premiers positifs sont

2, 3, 5, 7, 11, 13, 17, 19, 23, 29;

les premiers facteurs premiers négatifs sont

—2, —3, —5, —7, —11, —13, —17, —19, —23, —29.

Factorisation des nombres entiers. Les entiers a et b sont dits *premiers entre eux* si tout diviseur commun de ces derniers vaut $+1$ ou -1.

PROPOSITION 1.2. *Si des entiers a et b sont premiers entre eux, il existe alors des entiers u, v tels que* $au + bv = 1$.

D é m o n s t r a t i o n. Considérons l'ensemble

$$I = \{ax + by \mid x, y \in \mathbf{Z}\}.$$

On voit sans peine que cet ensemble n'est pas vide et est fermé par rapport à l'addition et à la multiplication par des entiers. I est donc un idéal de l'anneau $\mathbf{Z}$ des entiers. L'ensemble I comprend le nombre a, $a = a\cdot 1 + b\cdot 0$ et le nombre b: $b = a\cdot 0 + b\cdot 1$. L'ensemble I contient des nombres positifs, car a et b sont premiers entre eux et, par suite, l'un au moins de ces nombres est différent de zéro. Notons d le plus petit nombre naturel positif appartenant à l'ensemble I. Alors, par définition de l'ensemble I, il existe des entiers u, v tels que $au + bv = d$. Selon le théorème 4.4.5, d est un commun diviseur des nombres a et b. a et b étant premiers entre eux et $d > 0$, il s'ensuit que $d = 1$. Ainsi, $au + bv = 1$. □

THÉORÈME 1.3. *Si le produit de deux entiers se divise par un nombre premier p, alors un au moins des facteurs admet p pour diviseur.*

D é m o n s t r a t i o n. Soit ab le produit des nombres entiers admettant p pour diviseur, a ne se divisant pas par p. a et p sont alors premiers entre eux. Selon la proposition 1.2, il existe des entiers u, v tels que $au + pv = 1$, d'où

$$abu + pbv = b.$$

ab se divisant par p il s'ensuit que $abu + pbv$ se divise par p, c'est-à-dire b admet p pour diviseur. □

THÉORÈME 1.4. *Si un produit de plusieurs entiers se divise par un nombre premier p, un au moins de ses facteurs admet alors p pour diviseur.*

D é m o n s t r a t i o n (s'effectue par récurrence sur le nombre des facteurs en s'appuyant sur le théorème 1.3). Supposons que le théorème est vrai pour n facteurs. Soit $p \mid (a_1 \ldots a_n \cdot a_{n+1})$; donc, $p \mid (a_1 \ldots a_n)\, a_{n+1}$. Selon le théorème 1.3, un au moins des deux nombres $a_1 \ldots a_n$ et a_{n+1} se divise par p. Si a_{n+1} ne se divise pas par p, le produit $a_1 \ldots a_n$, par contre, se divise par p. Par conséquent, selon l'hypothèse de récurrence, un au moins des nombres $a_1 \ldots a_n$ se divise par p. □

THÉORÈME 1.5. *Tout entier positif différent de* 1 *peut être représenté sous forme de produit de facteurs premiers positifs. Cette représentation est unique à l'ordre des facteurs près.*

Démonstration. Soit a un entier positif différent de 1. Démontrons la représentabilité de a sous forme de produit de facteurs premiers positifs en admettant que cette proposition est vraie pour tous les entiers positifs autres que 1 et inférieurs à a. Si a est premier, la proposition est vraie. Si a est un nombre composé, on peut le représenter sous forme de produit bc des entiers b, c inférieurs à a et supérieurs à l'unité. Selon l'hypothèse de récurrence, b et c peuvent être représentés sous forme de produit des facteurs premiers positifs:

$$b = p_1 \ldots p_r, \qquad c = p_{r+1} \ldots p_m.$$

En portant ces factorisations dans l'égalité $a = bc$, on aboutit à la représentation du nombre a

$$a = p_1 \ldots p_r p_{r+1} \ldots p_m$$

sous forme d'un produit de facteurs premiers positifs.

Démontrons l'unicité de cette représentation en nous servant de la méthode de récurrence. Si a est premier, alors l'unicité de la représentation découle apparemment de la définition du nombre premier. Supposons que pour tous nombres inférieurs à a l'unicité de la représentation est respectée. a étant supposé composé, considérons deux représentations quelconques du nombre a sous forme de produit de facteurs premiers positifs:

$$(1) \qquad a = p_1 \ldots p_m = q_1 \ldots q_n.$$

Vu que $p_1 \mid q_1 \ldots q_n$, selon le théorème 1.4, au moins un des facteurs $q_1 \ldots q_n$ est divisible par p_1; pour un numérotage adéquat, on peut admettre que $p_1 \mid q_1$. Puisque p_1 et q_1 sont des facteurs premiers positifs, il s'ensuit que $p_1 = q_1$. En simplifiant les deux membres de l'égalité (1) par p_1 et en posant $a/p_1 = a_1$, il vient

$$a_1 = p_2 \ldots p_m = q_2 \ldots q_n.$$

Comme le nombre a_1 est inférieur à a, par hypothèse de récurrence, a_1 possède une représentation unique sous forme de produit de facteurs premiers positifs; donc, $m = n$ et, pour un numérotage adéquat, $p_2 = q_2, \ldots, p_m = q_m$. Le nombre a possède ainsi une représentation unique sous forme de produit de facteurs premiers positifs. □

COROLLAIRE 1.6. *Tout entier c différent de zéro et de* ± 1 *se représente de façon unique sous forme du produit*

$$(1) \qquad c = \varepsilon p_1 \ldots p_m,$$

où $p_1 \ldots p_m$ sont des nombres premiers positifs et $\varepsilon = \pm 1$.

Dans la représentation (1) peuvent apparaître des nombres premiers identiques. Si l'on réunit des facteurs premiers identiques dans la représentation (1) et l'on modifie, si nécessaire, le numérotage, on peut représenter (1) sous la forme

(2) $c = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$,

où $p_1, \ldots, p_s$ sont des nombres premiers distincts, $\varepsilon = \pm 1$ et $\alpha_i > 0$ pour $i = 1, 2, \ldots, s$. La représentation d'un entier (différent de zéro) sous forme (2) est appelée sa *factorisation canonique.*

Diviseurs d'un nombre entier. En connaissant la factorisation canonique d'un nombre naturel, on est en mesure de décrire les diviseurs de ce nombre.

PROPOSITION 1.7. *Soient n un nombre naturel et*

(1) $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_s^{\alpha_s}$

sa factorisation canonique. Alors, chaque diviseur naturel d du nombre n peut être écrit sous forme

(2) $d = p_1^{\delta_1} p_2^{\delta_2} \ldots p_s^{\delta_s}$,

où δ_i sont des entiers satisfaisant aux conditions

(3) $\delta_i \in \{0, 1, \ldots, \alpha_i\}$ pour $i = 1, 2, \ldots, s$.

D é m o n s t r a t i o n. Soit d un diviseur naturel quelconque du nombre n. Etant donné que chaque diviseur premier du nombre d est un diviseur du nombre n, dans la factorisation de d, en raison de (1), on ne peut rencontrer que des nombres de l'ensemble $\{p_1, \ldots \ldots, p_s\}$. Aussi le nombre d peut-il être représenté sous forme (2), les exposants δ_i satisfaisant aux conditions (3).

D'autre part, si d acquiert la représentation (2) et les exposants δ_i satisfont aux conditions (3), on a

$$n = d\,(p_1^{\alpha_1-\delta_1} \ldots p_s^{\alpha_s-\delta_s}) \qquad (\alpha_i - \delta_i \geqslant 0),$$

c'est-à-dire d est un diviseur naturel du nombre n.

Nombre et somme des diviseurs naturels d'un nombre. La proposition 1.7 permet de calculer le nombre et la somme des diviseurs naturels d'un nombre.

PROPOSITION 1.8. *Soit $n = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ la factorisation canonique du nombre naturel n. Alors le nombre $\tau(n)$ des diviseurs naturels du nombre n s'exprime par la formule $\tau(n) = (\alpha_1 + 1) \ldots (\alpha_s + 1)$.*

D é m o n s t r a t i o n. Selon la proposition 1.7, tout diviseur naturel d du nombre n peut être représenté sous forme

$$d = p_1^{\delta_1} \ldots p_s^{\delta_s},$$

où

(3) $\delta_i \in \{0, 1, \ldots, \alpha_i\}$ pour $i = 1, 2, \ldots, s$.

Aussi pour trouver le nombre de tous les diviseurs naturels du nombre n suffit-il de calculer le nombre de toutes les collections ordonnées $\delta_1, \ldots, \delta_s$ satisfaisant aux conditions (3). En raison de (3) δ_i peut prendre $\alpha_i + 1$ valeurs, les choix des différentes valeurs de $\delta_1, \ldots, \delta_s$ étant indépendants l'un de l'autre et, en vertu de l'unicité de la factorisation, à des collections différentes correspondent des diviseurs n distincts. Par conséquent, le nombre de tous les diviseurs naturels du nombre n vaut $(\alpha_1 + 1) \ldots (\alpha_s + 1)$.

Exemples. 1. Soit $n = 180$. Alors, $180 = 2^2 \cdot 3^2 \cdot 5$ et

$$\tau(180) = (2 + 1)(2 + 1)(1 + 1) = 18.$$

2. Soit $n = 60$. Alors, $60 = 2^2 \cdot 3 \cdot 5$ et

$$\tau(60) = (2 + 1)(1 + 1)(1 + 1) = 12.$$

Proposition 1.9. *Soit $n = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ la factorisation canonique du nombre naturel n. La somme $\sigma(n)$ de tous les diviseurs naturels du nombre n s'exprime alors par la formule*

$$(4) \quad \sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_s^{\alpha_s+1} - 1}{p_s - 1}.$$

Démonstration. Selon la proposition 1.7, chaque diviseur du nombre n prend la forme $p_1^{\delta_1} \ldots p_s^{\delta_s}$ et

$$(5) \quad \sigma(n) = \sum_{\substack{\delta_1 \in \{0, 1, \ldots, \alpha_1\} \\ \cdots\cdots \\ \delta_s \in \{0, 1, \ldots, \alpha_s\}}} p_1^{\delta_1} \ldots p_s^{\delta_s}.$$

On voit aisément que chaque terme de la somme dans (5) se rencontre exactement une fois après suppression des parenthèses du produit

$$(6) \quad (1 + p_1 + \ldots + p_1^{\alpha_1}) \ldots (1 + p_s + \ldots + p_s^{\alpha_s}).$$

La somme (5) est donc égale au produit (6). Chaque facteur étant une somme des termes d'une progression géométrique, le produit (6) vaut

$$\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_s^{\alpha_s+1} - 1}{p_s - 1}.$$

La formule (4) est donc vérifiée. □

Exemple. Soit $n = 60$. Alors $n = 2^2 \cdot 3 \cdot 5$ et

$$\sigma(60) = \frac{2^3 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 7 \cdot 4 \cdot 6 = 168.$$

Ensemble infini des nombres premiers. Le théorème suivant a été démontré par Euclide.

Théorème 1.10. *Un ensemble des nombres premiers positifs est infini.*

D é m o n s t r a t i o n. Montrons que pour chaque ensemble fini donné des nombres premiers positifs $p_1, \ldots, p_n$ il existe un nombre premier positif différent de tous les nombres de cet ensemble. A cette fin, considérons le nombre

$$a = p_1 \cdot p_2 \ldots p_n + 1.$$

a étant un nombre naturel supérieur à l'unité, selon le théorème 1.5, on peut le décomposer en un produit de facteurs premiers positifs et, de ce fait, il a au moins un diviseur premier positif p. Ce diviseur diffère de $p_1 \cdot p_2, \ldots, p_n$, car, dans le cas contraire, $p \mid p_1 \ldots \ldots p_n$, $p \mid a$ et la différence $a - p_1 \cdot p_2 \ldots p_n = 1$ se diviserait par p, or c'est impossible. Par conséquent, l'ensemble de tous les premiers est infini. □

Crible d'Eratosthène. Etudions la méthode d'obtention des premiers positifs ne dépassant pas un nombre donné.

PROPOSITION 1.11. *Un nombre composé positif a possède au moins un diviseur premier positif ne dépassant pas $\sqrt{a}$.*

D é m o n s t r a t i o n. Parmi les diviseurs positifs du nombre a différents de l'unité il existe un plus petit; désignons-le par p. Si le nombre p était composé, il comporterait un diviseur positif q satisfaisant aux conditions $1 < q < p$. Dans ce cas le nombre q serait un diviseur positif du nombre a inférieur à p, ce qui est en contradiction avec le choix du nombre p. Donc, p est un nombre premier. Si $a = pb$, alors $b \geqslant p$. En multipliant membre à membre $a = pb$ et $b \geqslant p$ et en simplifiant par b, on obtient $a \geqslant p^2$ et $p \leqslant \leqslant \sqrt{a}$.

PROPOSITION 1.12. *Si un nombre positif a différent de l'unité ne se divise par aucun nombre premier positif ne dépassant pas $\sqrt{a}$, il est alors premier.*

Cette proposition découle directement de la proposition 1.11. Il existe une méthode simple de construction du tableau des nombres premiers positifs ne dépassant pas un entier donné. Cette méthode porte le nom de *crible d'Eratosthène*.

Supposons qu'il s'agit de trouver tous les premiers positifs ne dépassant pas un nombre naturel a. A cette fin, écrivons la suite de tous les nombres naturels de 2 à a: 2, 3, 4, . . ., a. Dans cette suite rayons chaque deuxième nombre après 2. Le premier nombre non supprimé est le nombre premier 3. Ensuite, biffons chaque troisième nombre après 3 (en comptant les nombres déjà rayés). Le premier nombre suivant 3 non biffé est le nombre premier 5. Eliminons chaque cinquième nombre après 5, etc. On continuera cette élimination tant qu'on n'atteigne le premier nombre premier non inférieur à $\sqrt{a}$. En vertu de la proposition 1.12, tous les nombres non rayés seront des premiers positifs ne dépassant pas a.

E x e m p l e. Construisons le tableau des premiers positifs ne dépassant pas 50. A cette fin écrivons les nombres naturels de 2 à 50 et procédons aux éliminations jusqu'à la rencontre du premier nombre supérieur ou égal à $\sqrt{50}$, c'est-à-dire jusqu'à 11 (les nombres rayés sont en caractères non gras):

2 **3** 4 **5** 6 **7** 8 9 10 **11** 12 **13** 14 15 16 **17** 18 **19** 20 21 22 **23**
24 25 26 27 28 **29** 30 **31** 32 33 34 35 36 **37** 38 39 40 **41** 42 **43**
44 45 46 **47** 48 49 50

Barrons dans cette suite chaque deuxième nombre après 2, ensuite chaque troisième après 3, ensuite chaque cinquième nombre après 5 et, enfin, chaque septième après le nombre 7. Tous les nombres restants seront premiers. On obtient ainsi le tableau suivant de la suite des nombres premiers positifs inférieurs à 50:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

Exercices

1. Montrer que pour tout entier n le nombre $n(n+1)(n+2)$ est divisible par 6.
2. Montrer que pour tout entier n le nombre $n(n+1)(2n+1)$ est divisible par 6.
3. Soient m et n des entiers premiers entre eux. Montrer que sont premiers entre eux les nombres suivants: m et $m+n$, m et $m-n$, $m+n$ et $2m+n$.
4. Soient a, b, c, d des entiers positifs et a/b, c/d des fractions irréductibles. Montrer que si $a/b = c/d$, alors $a = c$ et $b = d$.
5. Montrer que si $2^n + 1$ est un nombre premier, alors $n = 2^m$.
6. Montrer que si $2^n - 1$ est un nombre premier, alors n est premier.
7. Soient a et n des entiers positifs, $a > 1$. Démontrer que si $a^n + 1$ est un nombre premier, alors $n = 2^m$.
8. Factoriser le nombre 50!
9. Montrer qu'avec un nombre naturel $n > 1$ la somme $1 + \frac{1}{2} + \ldots + \frac{1}{n}$ ne peut être un nombre entier.
10. Un nombre naturel est dit *parfait* s'il est égal à la moitié de la somme de ses diviseurs positifs. Démontrer que tout nombre pair parfait est de la forme $2^n(2^{n+1} - 1)$, où $n \in \mathbf{N}$, avec $2^{n+1} - 1$ premier.

§ 2. Plus grand commun diviseur et plus petit commun multiple

Plus grand commun diviseur. Un entier c est dit *diviseur commun des entiers* $a_1, \ldots, a_n$ si c divise chacun de ces nombres.

DÉFINITION. On appelle *plus grand commun diviseur des entiers* $a_1, \ldots, a_n$ un commun diviseur divisible par tout commun diviseur de ces nombres. Des entiers $a_1, \ldots, a_n$ sont dits *premiers entre eux* si leur plus grand commun diviseur vaut l'unité.

Un plus grand commun diviseur des nombres $a_1, \ldots, a_n$ est noté PGCD $(a_1, \ldots, a_n)$; un plus grand commun diviseur positif de ces nombres est noté pgcd $(a_1, \ldots, a_n)$.

COROLLAIRE 2.1. *Si d est un plus grand commun diviseur des entiers $a_1, \ldots, a_n$, l'ensemble de tous les diviseurs communs de ces nombres coïncident alors avec l'ensemble de tous les diviseurs du nombre d.*

COROLLAIRE 2.2. *Deux quelconques plus grands communs diviseurs des entiers $a_1, \ldots, a_n$ sont associatifs, c'est-à-dire ne peuvent différer que de signe. Si d est un plus grand commun diviseur des nombres $a_1, \ldots, a_n$, alors le nombre $(-d)$ est également un plus grand commun diviseur de ces nombres.*

PROPOSITION 2.3. *Si* $a = \prod_{p \mid a} p^{\alpha_p}$ et $b = \prod_{p \mid b} p^{\beta_p}$ *sont des factorisations canoniques des entiers positifs a et b, le nombre*

$$d = \prod_{\substack{p \mid a \\ p \mid b}} p^{\min(\alpha_p,\, \beta_p)}$$

est alors le plus grand commun diviseur des nombres a et b.

Démonstration. Le nombre d est un diviseur de a comme de b en vertu de la proposition 1.7, autrement dit, d est le commun diviseur de a et b. Ensuite, si c est un commun diviseur quelconque positif de a et b, en vertu de la proposition 1.7,

$$c = \prod_{\substack{p \mid a \\ p \mid b}} p^{\gamma_p},$$

de plus, pour chaque diviseur de a et b, on a les inégalités $\gamma_p \leqslant \alpha_p$, $\gamma_p \leqslant \beta_p$. Donc, $c \mid d$. Par conséquent, d est un plus grand commun diviseur des nombres a et b. □

Soient $a_1, \ldots, a_n$ des entiers quelconques. Considérons l'ensemble

$$(1) \quad I = \{k_1 a_1 + \ldots + k_n a_n \mid k_1, \ldots, k_n \in \mathbf{Z}\}$$

de toutes les combinaisons linéaires entières des nombres $a_1, \ldots, a_n$. On vérifie sans peine que cet ensemble est l'idéal de l'anneau $\mathbb{Z}$. Cet idéal est appelé *idéal engendré par les nombres* $a_1, \ldots, a_n$ et noté $(a_1, \ldots, a_n)$.

THÉORÈME 2.4. *Pour toute collection d'entiers $a_1, \ldots, a_n$ il existe un plus grand commun diviseur. Le nombre d est un plus grand commun diviseur des nombres $a_1, \ldots, a_n$ si et seulement si l'idéal $(a_1, \ldots, a_n)$ est égal à l'idéal (d).*

Démonstration. Si tous les nombres $a_1, \ldots, a_n$ sont égaux à zéro, l'unique plus grand commun diviseur de ces nombres est le nombre zéro.

Supposons qu'au moins un des nombres $a_1, \ldots, a_n$ est différent de zéro. Considérons l'ensemble I de toutes les combinaisons linéaires entières des nombres $a_1, \ldots, a_n$. L'ensemble I comprend les nombres a_s, $s = 1, \ldots, n$, car $a_s = k_1a_1 + \ldots + k_na_n$, où $k_s = 1$ et $k_i = 0$ pour $i \neq s$. Aussi l'ensemble I comprend-il des nombres différents de zéro. L'ensemble I est l'idéal de l'anneau des entiers engendré par les nombres $a_1, \ldots, a_n$; $I = (a_1, \ldots, a_n)$. Selon le théorème 4.4, chaque idéal de l'anneau $\mathbb{Z}$ est principal et, par suite, est composé de multiples d'un certain nombre entier d, $I = d\mathbb{Z}$. Démontrons que d est PGCD $(a_1, \ldots, a_n)$. Comme chaque élément de l'ensemble I se divise par d, on a $d \mid a_i$ pour $i = 1, \ldots, n$, c'est-à-dire que d est un diviseur commun des nombres $a_1, \ldots, a_n$. Ensuite, comme $d \in I$, selon (1), il existe des entiers $k_1, \ldots, k_n$ tels que

$$d = k_1a_1 + \ldots + k_na_n.$$

Il s'ensuit que tout diviseur commun c des nombres $a_1, \ldots, a_n$ est également un diviseur du nombre d. Ainsi, tout élément d engendrant l'idéal $I = (a_1, \ldots, a_n)$ est un plus grand commun diviseur des nombres $a_1, \ldots, a_n$. Il s'ensuit, en particulier de la démonstration, que toute collection finie des nombres $a_1, \ldots, a_n$ possède un plus grand commun diviseur.

Soient d' un quelconque plus grand commun diviseur des nombres $a_1, \ldots, a_n$ et d, comme toujours, un nombre engendrant l'idéal I; démontrons que $(a_1, \ldots, a_n) = (d')$. Tous deux PGCD des nombres $a_1, \ldots, a_n$ sont associatifs, c'est-à-dire ne diffèrent que par le signe. Par suite, $d' = \pm d$. Donc, l'idéal (d') coïncide avec l'idéal (d). Par conséquent, $(a_1, \ldots, a_n) = (d')$. □

L'analyse de la démonstration du théorème précédent permet également de formuler le théorème suivant.

THEOREME 2.5. *Représentons le plus grand commun diviseur d des entiers $a_1, \ldots, a_n$ sous forme d'une combinaison linéaire entière de ces nombres, c'est-à-dire sous forme $d = k_1a_1 + \ldots + k_na_n$ aux entiers $k_1, \ldots, k_n$. Ceci étant, si les nombres $a_1, \ldots, a_n$ ne sont pas tous nuls, alors $\mid d \mid$ est le plus petit entier positif représentable sous cette forme. Tous les nombres représentés sous cette forme, autrement dit, tous les nombres de l'idéal $(a_1, \ldots, a_n)$ sont multiples du nombre d.*

PROPOSITION 2.6. *Si un diviseur commun d des entiers $a_1, \ldots, a_n$ se représente sous forme d'une combinaison linéaire entière de ces nombres, d est alors un plus grand commun diviseur des nombres $a_1, \ldots, a_n$.*

Démonstration. Supposons que le diviseur commun d des nombres $a_1, \ldots, a_n$ se représente sous forme

$$d = k_1a_1 + \ldots + k_na_n,$$

où $k_1, \ldots, k_n$ sont des entiers. Dans ce cas tout diviseur commun des nombres $a_1, \ldots, a_n$ divise la somme $k_1a_1 + \ldots + k_na_n$ et, partant, d. Donc d est un plus grand commun diviseur des nombres $a_1, \ldots, a_n$. □

PROPOSITION 2.7. *Pour tous entiers a, b, c*

$$\text{PGCD}\,(a, b, c) \sim \text{PGCD}\,(\text{PGCD}\,(a, b), c).$$

Démonstration. Soient d_1, PGCD (a, b) et d, PGCD (d_1, c). Alors d est un diviseur commun des nombres d_1 et c, tandis que le nombre d_1 est un diviseur commun des nombres a et b. Donc, d est un diviseur commun des nombres a, b et c. Selon le théorème 2.5, les nombres d et d_1 peuvent être représentés sous forme

$$d = kd_1 + k_3c, \quad d_1 = k_1a + k_2b,$$

où k, k_1, k_2, k_3 sont des entiers; aussi a-t-on $d = kk_1a + kk_2b + k_3c$. Ainsi, le diviseur commun d des nombres a, b, c peut être exprimé linéairement au moyen de ces nombres. Par conséquent, selon la proposition 2.6, d est un plus grand commun diviseur de ces nombres. □

Cette proposition permet de réduire la recherche du plus grand commun diviseur de plusieurs nombres à la recherche du plus grand commun diviseur de deux nombres.

PROPOSITION 2.8. *Pour des entiers quelconques a, b et c*

$$\text{PGCD}\,(ac, bc) \sim c\cdot\text{PGCD}\,(a, b).$$

Démonstration. Soit d un PGCD (a, b). Alors, selon le théorème 2.5, d peut être représenté sous forme

$$d = k_1a + k_2b,$$

où k_1 et k_2 sont des entiers, donc $cd = k_1ac + k_2bc$. En outre, comme d est le diviseur commun de a et b, cd l'est de ac et bc. Par conséquent, selon la proposition 2.6, le nombre cd est un plus grand commun diviseur de ac et bc. □

Nombres premiers entre eux. Etudions les propriétés des nombres premiers entre eux.

PROPOSITION 2.9. *Des nombres entiers $a_1, \ldots, a_n$ sont premiers entre eux si et seulement si l'unité se représente sous forme d'une combinaison linéaire entière de ces nombres.*

Démonstration. Si les nombres $a_1, \ldots, a_n$ sont premiers entre eux, leur plus grand commun diviseur, l'unité, se représente, selon le théorème 2.5, sous forme d'une combinaison linéaire entière de ces nombres.

Inversement, si l'unité se représente sous forme d'une combinaison linéaire entière des nombres $a_1, \ldots, a_n$, alors, en vertu de la proposition 2.6, l'unité est un plus grand commun diviseur de ces nombres. Aussi les nombres $a_1, \ldots, a_n$ sont-ils premiers entre eux. □

PROPOSITION 2.10. *Des entiers $a_1, \ldots, a_n$ sont premiers entre eux si et seulement s'ils ne possèdent pas de diviseur premier commun.*

La démonstration est laissée au soin du lecteur.

THÉORÈME 2.11. *Si un nombre entier divise le produit de deux entiers et est premier avec l'un des facteurs, alors il divise l'autre facteur.*

Démonstration. Soient a et b deux premiers entre eux et a divise bc. Démontrons que a divise c. a et b étant premiers entre eux, il existe des entiers k_1 et k_2, tels que

$$k_1a + k_2b = 1.$$

En multipliant les deux membres de l'égalité par c, il vient $k_1ac + k_2bc = c$. De plus, a divise bc. Donc, a divise $k_1ac + k_2bc$, c'est-à-dire a divise c. □

PROPOSITION 2.12. *Un diviseur commun d des entiers $a_1, \ldots, a_n$ non simultanément nuls est leur plus grand commun diviseur si et seulement si $a_1/d, \ldots, a_n/d$ sont premiers entre eux.*

Démonstration. Vu que par hypothèse les nombres $a_1, \ldots, a_n$ ne sont pas tous nuls, on a $d \neq 0$. Si d est le plus grand commun diviseur des nombres $a_1, \ldots, a_n$, alors, selon le théorème 2.5, il peut être exprimé linéairement au moyen de $a_1, \ldots, a_n$:

$$k_1a_1 + \ldots + k_na_n = d, \tag{1}$$

où $k_1, \ldots, k_n$ sont des entiers. En divisant les deux membres de l'égalité par d, il vient

$$k_1\frac{a_1}{d} + \ldots + k_n\frac{a_n}{d} = 1. \tag{2}$$

De là, selon la proposition 2.9, il s'ensuit que les nombres $a_1/d, \ldots$ $\ldots, a_n/d$ sont premiers entre eux.

Inversement: si les nombres $a_1/d, \ldots, a_n/d$ sont premiers entre eux, alors, selon la proposition 2.9, il existe des entiers $k_1, \ldots$ $\ldots, k_n$ pour lesquels est satisfaite l'égalité (2). En multipliant les deux membres de cette égalité par d, on obtient l'égalité (1). Vu que le diviseur commun d des nombres $a_1, \ldots, a_n$ se représente sous forme d'une combinaison linéaire de ces nombres, selon la proposition 2.6, le nombre d est un plus grand diviseur de $a_1, \ldots$ $\ldots, a_n$. □

Plus petit commun multiple. L'entier c est appelé *multiple commun des entiers* $a_1, \ldots, a_n$ s'il est divisible par chacun de ces nombres.

DÉFINITION. On appelle *plus petit commun multiple des entiers* $a_1, \ldots, a_n$ un tel multiple commun qui divise tout multiple commun de ces nombres. Un plus petit commun multiple des entiers $a_1, \ldots, a_n$ est noté PPCM $(a_1, \ldots, a_n)$. Un plus petit commun multiple positif des nombres $a_1, \ldots, a_n$ différents de zéro est noté $[a_1, \ldots, a_n]$.

De la définition du PPCM $(a_1, \ldots, a_n)$ on tire directement le corollaire.

COROLLAIRE 2.13. *Deux plus petits communs multiples quelconques des nombres* $a_1, \ldots, a_n$ *sont associatifs dans* $\mathbb{Z}$, *c'est-à-dire ne diffèrent que du signe. Si* m *est* PPCM $(a_1, \ldots, a_n)$, *le nombre* $(-m)$ *est aussi* PPCM $(a_1, \ldots, a_n)$.

COROLLAIRE 2.14. *Si* m *est un plus petit commun multiple des nombres* $a_1, \ldots, a_n$, *alors l'ensemble de tous les multiples communs de ces nombres coïncide avec l'ensemble de tous les multiples du nombre* m.

PROPOSITION 2.15. *Soient* $a = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ *et* $b = p_1^{\beta_1} \ldots \ldots p_s^{\beta_s}$, *où* $p_1, \ldots, p_s$ *sont des nombres positifs différents deux à deux premiers entre eux et* α_i, β_i *des entiers non négatifs. Alors*

$$[a, b] = p^{\max(\alpha_1, \beta_1)} \ldots p_s^{\max(\alpha_s, \beta_s)}.$$

La démonstration de cette proposition est laissée au soin du lecteur.

THÉORÈME 2.16. *Pour toute collection d'entiers* $a_1, \ldots, a_n$ *il existe un plus petit commun multiple. L'entier* m *est* PPCM $(a_1, \ldots \ldots, a_n)$ *si et seulement si* $(a_1) \cap \ldots \cap (a_n) = (m)$, *où* (a_i) *est l'idéal engendré par le nombre* a_i.

D é m o n s t r a t i o n. Considérons l'ensemble

$$(1) \quad I = (a_1) \cap \ldots \cap (a_n).$$

Vu que les ensembles $(a_1), \ldots, (a_n)$ sont fermés par rapport à l'addition et à la multiplication par des entiers, il est aisément vérifiable que leur intersection I est également fermée par rapport à l'addition et à la multiplication par des entiers. En outre, cet ensemble n'est pas vide, puisqu'il comporte un zéro. Donc, I est un idéal de l'anneau des entiers. Selon le théorème 4.4, tout idéal de l'anneau des entiers est principal, c'est-à-dire il existe un entier m, tel que chaque nombre de I soit multiple de m, $I = (m)$. Démontrons que m est PPCM $(a_1, \ldots, a_n)$. Comme $m \in I$, alors, selon (1), $m \in (a_i)$ pour $i = 1, \ldots, m$, c'est-à-dire m est un plus petit commun multiple des nombres $a_1, \ldots, a_n$. De plus, si m' est un multiple commun quelconque des nombres $a_1, \ldots, a_n$, on a alors $m' \in \in (a_1), \ldots, m' \in (a_n)$. Par conséquent, $m' \in I = (a_1) \cap \ldots \cap (a_m) = = (m)$ et, par suite, m' est divisible par m. Ainsi, m est un plus petit commun multiple des nombres $a_1, \ldots, a_n$.

Supposons maintenant que m_1 est un plus petit commun multiple des nombres $a_1, \ldots, a_n$ et démontrons que $(m_1) = (a_1) \cap \ldots \ldots \cap (a_n)$. Comme les nombres m_1 et m sont des plus petits communs multiples d'une même collection de nombres $a_1, \ldots, a_n$, ils sont donc associatifs dans $\mathbb{Z}$, c'est-à-dire $m_1 = \pm m$. Par conséquent, $(m_1) = (m)$ et, partant, $(a_1) \cap \ldots \cap (a_n) = (m_1)$. □

PROPOSITION 2.17. *Pour tous entiers a, b et c différents de zéro avec $c > 0$, on a*: $[ac, bc] = c\,[a, b]$.

D é m o n s t r a t i o n. Soit $m = [a, b]$. Vu que m est un multiple commun de a et b, cm est un multiple commun des nombres ac et bc. Soit m' un multiple commun quelconque des nombres ac et bc, c'est-à-dire

$$m' = kac = sbc,$$

où k et s sont des entiers. Comme $c \neq 0$, $ka = sb$. Donc, ka est divisible par m et, partant, m' est divisible par mc. Ainsi, cm est un plus petit commun multiple des nombres ac et bc. En outre, $cm > 0$; donc $[ac, bc] = cm = c\,[a, b]$. □

COROLLAIRE 2.18. *Pour tous entiers a, b et c différents de zéro* PPCM $(ac, bc) \sim c\cdot$PPCM (a, b).

PROPOSITION 2.19. *Si des entiers a et b sont premiers entre eux, ab est alors un plus petit commun multiple des nombres a et b.*

D é m o n s t r a t i o n. Le nombre ab est un multiple commun de a et b. Aussi est-il suffisant de démontrer que tout multiple commun m des nombres a et b est divisible par ab. Le nombre m est multiple de b, c'est-à-dire $m = bc$, où c est un entier, et $a \mid bc$. Comme, par hypothèse, a et b sont premiers entre eux il s'ensuit, selon le théorème 2.11, que a divise c, $c = ad$. Par conséquent, $m = abd$, c'est-à-dire m est divisible par ab. Ainsi, ab est un plus petit commun multiple des nombres a et b. □

PROPOSITION 2.20. *Si des entiers a et b sont différents de zéro, on a*

$$(1) \quad \text{PPCM}\,(a, b) \sim \frac{ab}{\text{PGCD}\,(a, b)}.$$

D é m o n s t r a t i o n. Soit d un plus grand commun diviseur des nombres a et b. a et b étant différents de zéro, on a $d \neq 0$. Selon le corollaire 2.18,

$$(2) \quad \text{PPCM}\,(a, b) \sim d\,\text{PPCM}\,(a/d, b/d).$$

Ensuite, en vertu de la proposition 2.12, PGCD $(a/d, b/d) = 1$. D'où, en raison de la proposition 2.19,

$$(3) \quad \text{PPCM}\left(\frac{a}{d}, \frac{b}{d}\right) \sim \frac{a}{d}\cdot\frac{b}{d}.$$

Sur la base de (2) et (3) on conclut que la relation (1) se vérifie. □

THÉORÈME 2.21. *Pour tous entiers a, b et c, on a*

$$(1) \quad \text{PPCM}\,(a, b, c) \sim \text{PPCM}\,(\text{PPCM}\,(a, b), c).$$

D é m o n s t r a t i o n. Soit $m =$ PPCM (a, b, c), $m_1 =$ PPCM (a, b) et $m' =$ PPCM (m_1, c). Selon le théorème 2.16, on a

$$(2) \quad (m) = (a) \cap (b) \cap (c), \quad (m_1) = (a) \cap (b), \quad (m') = (m_1) \cap (c);$$

donc

(3) $(m') = ((a) \cap (b)) \cap (c) = (a) \cap (b) \cap (c)$.

De (2) et (3) il s'ensuit que $(m) = (m')$. □

Exercices

1. Soient a et b des entiers positifs premiers entre eux. Montrer que la somme $\frac{1}{a} + \frac{1}{a+b}$ après réduction au même dénominateur est une fraction irréductible.

2. Démontrer que d est un plus grand commun diviseur des entiers a, b, c si et seulement si a/d, b/d, c/d sont des entiers premiers entre eux.

3. Démontrer que pour des entiers quelconques a, b, c, k PGCD $(ka, kb, kc) \sim k$ PGCD (a, b, c).

4. Démontrer que le multiple commun m des entiers a, b, c est un plus petit commun multiple si et seulement si les nombres m/a, m/b, m/c sont premiers entre eux $(a, b, c \neq 0)$.

5. Soit $\alpha = m/n$, où m, n sont des entiers premiers entre eux, $m \neq 0$ et $n > 0$. Si $\alpha = r/s$, où r, s sont des entiers et $s > 0$, il existe alors un nombre naturel t, tel que $r = tm$ et $s = tn$. De plus, t est un plus grand commun diviseur des nombres r et s.

§ 3. Algorithme d'Euclide et fractions continues finies

Algorithme d'Euclide. Etudions le plus simple des procédés d'obtention du plus grand commun diviseur de deux entiers.

Proposition 3.1. *Soient a et b deux entiers, $b \neq 0$ et*

(1) $a = bq + r \qquad (0 \leqslant r < |b|)$.

Alors pgcd (a, b) = pgcd (b, r).

Démonstration. Il s'ensuit de (1) que tout diviseur commun des nombres a et b est un diviseur du nombre $r = a - bq$ et que tout diviseur commun des nombres b et r est un diviseur du nombre a. L'ensemble de tous les diviseurs communs des nombres a et b coïncide donc avec l'ensemble de tous les diviseurs communs des nombres b et r. Il s'ensuit que le diviseur commun positif des nombres a et b coïncide avec le diviseur commun positif des nombres b et r, c'est-à-dire pgcd (a, b) = pgcd (b, r). □

Si $b \mid a$, où $b \geqslant 1$, il est évident que pgcd $(a, b) = b$. Pour trouver le pgcd de deux nombres entiers on se sert du procédé de *division successive* dénommé *algorithme d'Euclide*. Le principe de ce procédé réside dans le fait qu'en vertu de la proposition démontrée plus haut le problème de la recherche du pgcd des nombres a et b se réduit à un problème plus simple de recherche du pgcd de b et r, où $0 \leqslant r < |b|$. Si $r = 0$, pgcd $(a, b) = b$. Si, par contre, $r \neq 0$, on reprend le raisonnement à partir de b et r. Finalement, on obtient

une suite d'égalités

$$
(2)\quad
\begin{array}{ll}
a = ba_0 + r_1, & 0 < r_1 < |b|, \\
b = r_1 a_1 + r_2, & 0 < r_2 < r_1, \\
\dots\dots\dots\dots\dots\dots\dots\dots & \\
r_{n-2} = r_{n-1} a_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\
r_{n-1} = r_n a_n + r_{n+1}. &
\end{array}
$$

On a obtenu une suite décroissante des nombres naturels

$$r_1 > r_2 > \dots > r_n > \dots \geqslant 0,$$

qui ne peut être infinie. Il existe donc un reste égal à zéro; soit $r_{n+1} = 0$, $r_n \neq 0$.

Sur la base de la proposition 3.1 à partir de l'égalité (2) on a pgcd (a, b) = pgcd (b, r_1) = pgcd $(r_1, r_2) = \dots =$ pgcd (r_{n-1}, r_n) = pgcd $(r_n, 0) = r_n$, c'est-à-dire r_n = pgcd (a, b). Bref, on aboutit à la déduction: si à des entiers a, b, où $b \neq 0$, on applique l'algorithme d'Euclide, alors le dernier reste non nul de cet algorithme est pgcd (a, b).

Fractions continues finies. Tout nombre rationnel peut être représenté sous forme de a/b, où a et b sont des entiers et $b \geqslant 1$. En appliquant à a et b l'algorithme d'Euclide, on obtient une suite d'égalités :

$$
\begin{aligned}
a &= ba_0 + r_1, \\
b &= r_1 a_1 + r_2, \\
r_1 &= r_2 a_2 + r_3, \\
&\dots\dots\dots\dots \\
r_{n-3} &= r_{n-2} a_{n-2} + r_{n-1}, \\
r_{n-2} &= r_{n-1} a_{n-1} + r_n, \\
r_{n-1} &= r_n a_n,
\end{aligned}
$$

où $b > r_1 > r_2 > \dots > r_{n-1} > r_n > 0$. Cette suite d'égalités peut s'écrire sous forme

$$
\begin{aligned}
\frac{a}{b} &= a_0 + \frac{r_1}{b}, \\
\frac{b}{r_1} &= a_1 + \frac{r_2}{r_1}, \\
\frac{r_1}{r_2} &= a_2 + \frac{r_3}{r_2}, \\
&\dots\dots\dots\dots \\
\frac{r_{n-2}}{r_{n-1}} &= a_{n-1} + \frac{r_n}{r_{n-1}}, \\
\frac{r_{n-1}}{r_n} &= a_n.
\end{aligned}
$$

En se servant de ces égalités, il est possible d'exprimer a/b au moyen des nombres $a_0, a_1, \ldots, a_n$. En effet, la première égalité peut s'écrire sous forme

$$\frac{a}{b} = a_0 + \frac{1}{\frac{b}{r_1}};$$

en substituant à b/r_1 son expression tirée de la seconde égalité, il vient

$$\frac{a}{b} = a_0 + \frac{1}{a_1 + \frac{r_2}{r_1}} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{r_1}{r_2}}},$$

etc. Finalement, on obtient

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{}{\ddots + \cfrac{1}{a_n}}}}.$$

L'expression se trouvant dans le second membre de cette égalité est appelée *fraction continue.*

DÉFINITION. On appelle *fraction continue finie* l'expression de la forme

$$(1) \qquad a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{}{\ddots + \cfrac{1}{a_n}}}},$$

où a_0 est un entier, $a_1, \ldots, a_n$ des entiers positifs et $a_n > 1$.

Habituellement, une fraction continue (1) s'écrit de façon abrégée ainsi:

$$| a_0;\ a_1,\ a_2,\ \ldots,\ a_n |.$$

Les raisonnements fournis plus haut montrent que tout nombre rationnel peut être représenté sous forme d'une fraction continue finie.

E x e m p l e. Développons en fraction continue le nombre $\frac{126}{37}$.

A l'aide de l'algorithme d'Euclide on obtient:

$$\frac{126}{37} = 3 + \frac{15}{37} = 3 + \frac{1}{\frac{37}{15}} = 3 + \frac{1}{2 + \frac{1}{\frac{15}{7}}} = 3 + \frac{1}{2 + \frac{1}{2 + \frac{1}{7}}}$$

ou

$$\frac{126}{37} = |3;\ 2,\ 2,\ 7|.$$

On peut montrer que tout nombre rationnel possède une unique représentation sous forme de fraction continue finie.

Réduites. Soit

$$(1)\qquad a_0 + \cfrac{1}{a_1 + \ddots} = |a_0;\ a_1,\ \ldots,\ a_n|$$

une fraction continue finie. La fraction continue

$$(2)\qquad A_k = |\,a_0;\ a_1,\ \ldots,\ a_k\,|,$$

où $k \in \{0, 1, \ldots, n\}$, est appelée *k-ième réduite* de la fraction (1). Par définition, la *réduite nulle* de la fraction (1) est le nombre $A_0 = a_0$. Notons que la $(k+1)$-ième réduite A_{k+1} peut être obtenue à partir de la k-ième réduite A_k par substitution à l'élément a_k de l'élément $a_k + \frac{1}{a_{k+1}}$.

Définissons les nombres P_k et Q_k $(k \in \{0, 1, \ldots, n\})$ par récurrence au moyen des formules suivantes:

$$(3)\qquad \begin{array}{ll} P_0 = a_0, & Q_0 = 1, \\ P_1 = a_0 a_1 + 1, & Q_1 = a_1, \\ \ldots\ldots\ldots & \ldots\ldots \\ P_k = P_{k-1} a_k + P_{k-2}, & Q_k = Q_{k-1} a_k + Q_{k-2} \end{array}$$

$$(k \in \{2, 3, \ldots, n\}).$$

THÉORÈME 3.2. *Pour toute réduite A_k de la fraction continue* (1), *on a l'égalité*

$$(4)\qquad A_k = \frac{P_k}{Q_k} \qquad (k = 0, 1, \ldots, n).$$

Démonstration. La formule (4) se démontre par récurrence sur k. A partir de la formule (3) il s'ensuit directement les égalités

$$A_0 = \frac{a_0}{1} = \frac{P_0}{Q_0},$$

$$A_1 = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{P_1}{Q_1},$$

c'est-à-dire que l'affirmation du théorème se vérifie pour $k = 0$ et $k = 1$. Ensuite,

$$A_2 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}} = \frac{(a_0 a_1 + 1)\, a_2 + a_0}{a_1 a_2 + 1} = \frac{P_1 a_2 + P_0}{Q_1 a_2 + Q_0}$$

signifie que l'affirmation du théorème se vérifie pour $k = 2$.

Supposons que l'affirmation du théorème est vraie pour la m-ième réduite, où $2 \leqslant m < n$, c'est-à-dire

(5) $$A_m = \frac{P_m}{Q_m},$$

et démontrons que l'affirmation du théorème se vérifie pour $(m+1)$-ième réduite. Sur la base des formules (3) l'égalité (5) peut être écrite sous forme

(6) $$A_m = \frac{P_{m-1}a_m + P_{m-2}}{Q_{m-1}a_m + Q_{m-2}}.$$

Substituons dans les deux membres de l'égalité (6) à l'élément a_m l'élément $a_m + \frac{1}{a_{m+1}}$. Cette substitution transforme A_m en A_{m+1} et, par suite, on obtient à partir de (6)

$$A_{m+1} = \frac{P_{m-1}\left(a_m + \frac{1}{a_{m+1}}\right) + P_{m-2}}{Q_{m-1}\left(a_m + \frac{1}{a_{m+1}}\right) + Q_{m-2}} = \frac{(P_{m-1}a_m + P_{m-2})\,a_{m+1} + P_{m-1}}{(Q_{m-1}a_m + Q_{m-2})\,a_{m+1} + Q_{m-1}}.$$

De là, en vertu de (3),

$$A_{m+1} = \frac{P_m a_{m+1} + P_{m-1}}{Q_m a_{m+1} + Q_{m-1}} = \frac{P_{m+1}}{Q_{m+1}}.$$

Ainsi, de la vérité de la formule (4), pour $k = m$, s'ensuit la vérité de cette formule pour $k = m + 1$. Donc la formule (4) est vraie pour tous $k \in \{0, 1, \ldots, n\}$.

Les nombres P_k et Q_k définis par les formules (3) sont respectivement appelés *numérateur* et *dénominateur de la k-ième réduite*. Les formules (3) fournissent une méthode commode de calcul successif des numérateurs P_k et des dénominateurs Q_k des réduites. Le calcul se simplifie s'il est mené suivant le schéma:

a_k		a_0	a_1	a_2	a_3	...	a_n
P_k	1	a_0	P_1	P_2	P_3	...	P_n
Q_k	0	1	Q_1	Q_2	Q_3	...	Q_n

E x e m p l e. Cherchons les réduites de la fraction continue $|2; 5, 7, 3|$:

a_k		2	5	7	3
P_k	1	2	11	79	248
Q_k	0	1	5	36	113

Ainsi, les réduites de la fraction continue $|2; 5, 7, 3|$ sont les fractions

$$A_0 = \frac{P_0}{Q_0} = \frac{2}{1}, \quad A_1 = \frac{P_1}{Q_1} = \frac{11}{5},$$

$$A_2 = \frac{P_2}{Q_2} = \frac{79}{36}, \quad A_3 = \frac{P_3}{Q_3} = \frac{248}{113}.$$

THÉORÈME 3.3. *Pour $k \in \{1, \ldots, n\}$ est satisfaite l'égalité*

(7) $\quad P_{k-1}Q_k - Q_{k-1}P_k = (-1)^k.$

D é m o n s t r a t i o n. Soit $\Delta_k = P_{k-1}Q_k - Q_{k-1}P_k$. Sur la base des formules (3) l'égalité (7) se vérifie pour $k = 1$:

(8) $\quad \Delta_1 = P_0Q_1 - Q_0P_1 = a_0a_1 - 1\,(a_0a_1 + 1) = -1.$

En outre, selon (3),

$$\Delta_k = P_{k-1}Q_k - Q_{k-1}P_k = P_{k-1}(Q_{k-1}a_k + Q_{k-2}) - $$
$$- Q_{k-1}(P_{k-1}a_k + P_{k-2}) = P_{k-1}Q_{k-2} - Q_{k-1}P_{k-2} = -\Delta_{k-1}$$
$$(k \in \{2, \ldots, n\}).$$

En vertu de (8), il s'ensuit que

$$\Delta_k = (-1)^k \text{ pour } k \in \{1, 2, \ldots, n\},$$

autrement dit, l'égalité (7) se vérifie. □

COROLLAIRE 3.4. *Les nombres P_k et Q_k sont premiers entre eux et, par suite, chaque fraction P_k/Q_k est irréductible.*

D é m o n s t r a t i o n. En raison de (7) tout facteur commun de P_k et Q_k est diviseur de l'unité. Donc, les nombres P_k, Q_k sont premiers entre eux et la fraction P_k/Q_k est irréductible. □

Il existe entre deux réduites successives une relation importante découlant de (7).

COROLLAIRE 3.5. *Pour $k \in \{1, \ldots, n\}$ se vérifie l'égalité*

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{(-1)^k}{Q_{k-1}Q_k}.$$

Exercices

1. En se servant de l'algorithme d'Euclide chercher:

a) PGCD (549, 387); b) PGCD (589, 343); c) PGCD (12 606, 64 994).

2. Développer en fraction continue les fractions ordinaires suivantes:

a) 2,3547, b) $\frac{99}{170}$.

3. Simplifier en se servant du développement en fraction continue $\alpha = \frac{7857}{9153}$.

4. Sachant que $3{,}141592653 < \pi < 3{,}141592654$, chercher les quatre premières réduites pour le nombre π.

5. Sachant que $e = 2{,}71828182845\ldots$, chercher les quatre premières réduites pour le nombre e.

6. Résoudre en nombres entiers les équations suivantes:

a) $5x + 4y = 3$; b) $7x - 19y = 5$; c) $12x - 7y = 15$.

§ 4. Entiers systématiques

Entiers systématiques. Soient g un nombre naturel supérieur à 1 et $M = \{0, 1, \ldots, g-1\}$. On dit que le nombre naturel a est écrit dans un système de position de base g si

(1) $a = a_s g^s + a_{s-1} g^{s-1} + \ldots + a_1 g + a_0,$

où s est un entier non négatif, $a_0, \ldots, a_s \in M$ et $a_s \neq 0$.

Si chaque nombre de l'ensemble $M = \{0, 1, \ldots, g-1\}$ est désigné par un symbole spécial, ces symboles sont alors appelés *chiffres du système g-naire de position.* La représentation (1) s'écrit alors sous forme simplifiée

$$a = (a_s a_{s-1} \ldots a_1)_g$$

et s'appelle *notation du système g-naire de position.* C'est ainsi que la notation

$$a = (2315)_{10} \text{ signifie que } a = 2\cdot 10^3 + 3\cdot 10^2 + 1\cdot 10 + 5,$$

la notation

$$b = (101001)_2 \text{ signifie que } b = 1\cdot 2^5 + 0\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 1.$$

THÉORÈME 4.1. *Soient g un nombre naturel donné supérieur à l'unité et $M = \{0, 1, \ldots, g-1\}$. Tout nombre naturel a est représentable de façon unique sous forme*

(1) $a = a_s g^s + a_{s-1} g^{s-1} + \ldots + a_1 g + a_0,$

où $a_i \in M$ et $a_s \neq 0$.

Démonstration. L'existence de la représentation (1) se démontre par récurrence sur a. Si $a = 1$ ou $a < g$ l'égalité $a = a$

est la représentation cherchée. Soit $a \geqslant g$; supposons que pour tous les nombres naturels inférieurs à a on a déjà établi la possibilité de représentation (1). Vu que $a \geqslant g$, en divisant a par g avec reste, il vient

(2) $a = bg + a_0$, où $a_0 \in M$ et $1 \leqslant b < a$.

Puisque $b < a$, selon l'hypothèse de récurrence, le nombre b est représentable sous forme

(3) $b = a_s g^{s-1} + \ldots + a_2 g + a_1$, où $a_1, \ldots, a_s \in M$ et $a_s \neq 0$.

En portant l'expression (3) de b dans le second membre de (2), on obtient la représentation pour le nombre a,

$$a = a_s g^s + \ldots + a_1 g + a_0, \text{ où } a_i \in M \text{ et } a_s \neq 0,$$

appelée *décomposition du nombre a en puissances du nombre g*.

Démontrons l'univocité de la représentation par récurrence sur a. Si $1 \leqslant a < g$, on voit sans peine qu'il y a univocité. Supposons que l'univocité est démontrée pour tous les nombres naturels inférieurs à a. Admettons qu'outre (1) il existe pour a une autre représentation:

(4) $a = a'_{s'} g^{s'} + \ldots + a'_1 g + a'_0$.

En vertu de (1) et (4), il vient

(5) $$a = g(a_s g^{s-1} + \ldots + a_2 g + a_1) + a_0 = \\ = g(a'_{s'} g^{s'-1} + \ldots + a'_2 g + a'_1) + a'_0.$$

De (5), en vertu de l'univocité de la division avec reste, il s'ensuit que

$$a_0 = a'_0$$
$$b = a_s g^{s-1} + \ldots + a_2 g + a_1 = a'_{s'} g^{s'-1} + \ldots + a'_2 g + a'_1.$$

Comme $b < a$, par l'hypothèse de récurrence, $s = s'$ et $a_i = a'_i$ pour $i = 1, \ldots, s$. □

Opérations arithmétiques sur des entiers systématiques. Si les nombres naturels sont écrits dans le système de numération décimale on utilise alors les règles d'addition et de soustraction en « colonnes ». Les opérations d'addition et de soustraction des entiers multivalents dans le système de numération g-naire s'effectuent suivant les mêmes règles que dans la numération décimale. Dans la numération g-naire, comme dans la décimale, en additionnant des nombres multivalents on additionne d'abord les unités, ensuite on passe à l'ordre suivant, etc., jusqu'à l'ordre dominant en présence. En outre, chaque fois que la somme d'un ordre antérieur est supérieure à la base g du système de numération ou lui est égale, il est nécessaire de faire un report à l'ordre suivant.

Les exemples suivants illustrent les opérations d'addition dans les systèmes de numération sextenaire et binaire:

$$\begin{array}{r} (4253)_6 \\ + \ (2542)_6 \\ \hline (11235)_6 \end{array} \qquad \begin{array}{r} (10011)_2 \\ + \ (11001)_2 \\ \hline (101100)_2 \end{array}$$

La soustraction dans la numération quinaire est illustrée par l'exemple

$$\begin{array}{r} (42044)_5 \\ - \ (23141)_5 \\ \hline (13403)_5 \end{array}$$

L'opération de multiplication des entiers multivalents en numération g-naire s'effectue suivant les mêmes règles que dans la numération décimale (« en colonnes »). En effectuant la multiplication il est commode de se servir des tables de multiplication. On a donné plus bas la table de multiplication du système de numération sextenaire. Chaque cellule de cette table contient le produit des nombres représentant les numéros de la ligne et de la colonne dont l'intersection est la cellule même, tous les nombres figurant dans le système de numération sextenaire.

L'exemple suivant sert d'illustration de la multiplication (« en colonnes ») dans le système de numération sextenaire:

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	10	12	14
3	0	3	10	13	20	23
4	0	4	12	20	24	32
5	0	5	14	23	32	41

$$\begin{array}{r} 235 \\ \times \ 343 \\ \hline 1153 \\ 1432 \\ 1153 \\ \hline 135213 \end{array}$$

Transfert des nombres d'un système de numération à l'autre. Supposons que le nombre a est écrit dans le système de numération m-naire. Cela signifie qu'il est représenté sous forme d'une somme:

$$a = b_k m^k + b_{k-1} m^{k-1} + \ldots + b_1 m + b_0. \tag{1}$$

Comment transcrire ce nombre dans un autre système quelconque, disons, dans le système g-naire? Cela signifie qu'il faut repré-

senter le nombre a sous forme

(2) $$a = a_s g^s + a_{s-1} g^{s-1} + \ldots + a_1 g + a_0.$$

Il nous faut pour cela trouver les coefficients $a_0, a_1, \ldots, a_s$ dont chacun est un chiffre allant de 0 à $g - 1$ inclus. Divisons le nombre a donné en numération m-naire par g, obtenons le reste a_0 et le quotient q_1. Ensuite divisons le quotient q_1 par g et obtenons le reste a_1 et le quotient q_2. L'opération est poursuivie jusqu'à ce qu'on n'obtienne un reste égal à zéro. Finalement, on obtient tous les chiffres $a_0, a_1, \ldots, a_s$ entrant dans la représentation g-naire (2) du nombre a.

En guise d'exemple étudions le transfert du nombre $a = (5\,3\,7\,8)_{10}$ dans le système de numération sextenaire. En le divisant par 6, on obtient le quotient 896 et le reste 2. Donc dans la numération sextenaire le dernier chiffre du nombre a est 2. Pour trouver le second chiffre divisons le quotient 896 par 6. On obtient le quotient 149 et le reste 2. Le deuxième chiffre en numération sextenaire du nombre a est donc 2. Ensuite, divisons 149 par 6, on obtient le quotient 24 et le reste 5. Ce reste est le troisième chiffre du nombre a dans la numération sextenaire. Enfin, divisons le quotient 24 par 6, on obtient le quotient 4 et 0 comme reste. Donc,

$$(5\ 3\ 7\ 8)_{10} = (4\ 0\ 5\ 2\ 2)_6.$$

Exercices

1. Former la table de multiplication du système de numération septenaire.
2. Démontrer que $A = (a_n a_{n-1} \ldots a_1 a_0)_{12}$ est divisible par 8 (par 9) si est divisible par 8 (9) le nombre $(a_1 a_0)_{12}$ formé avec ses deux derniers chiffres.
3. Montrer que le nombre $A = (a_n a_{n-1} \ldots a_1 a_0)_g$, c'est-à-dire le nombre $a_n g^n + a_{n-1} g^{n-1} + \ldots + a_1 g + a_0$ est divisible par $g - 1$ si $g - 1$ est divisible par la somme de ses chiffres, c'est-à-dire la somme $a_n + a_{n-1} + \ldots + a_1 + a_0$.
4. Démontrer qu'un nombre naturel dont la numération décimale est composée de 3^n unités est divisible par 3^n.
5. Dans la numération décimale d'un nombre naturel il y a 30 unités, les chiffres restants étant des zéros. Ce nombre peut-il être un carré parfait?
6. Vous voulez connaître le numéro de mon téléphone par des questions auxquelles je ne répondrais que par des « oui » et « non ». Trouver le procédé garantissant le succès pour le plus petit nombre possible de questions (le numéro du téléphone est composé de cinq chiffres arbitraires).

§ 5. Distribution des nombres premiers

Distribution des nombres premiers. Désignons par $\pi(x)$ le nombre des premiers positifs inférieurs au nombre réel x. Il a été établi au § 1 qu'il existe une infinité de nombres premiers (théorème d'Euclide). Par conséquent, $\pi(x) \to \infty$ pour $x \to \infty$.

En 1808 Le Gendre publia la formule empirique qu'il avait trouvée pour la représentation approchée de la fonction $\pi(x)$. Le

Gendre énonça la proposition que pour des grandes valeurs de x $\pi(x)$ vaut approximativement $\frac{x}{\log x - 1,08366}$.

Tchébychev montra en 1849 le défaut de cette affirmation. Dans les travaux publiés en 1848 et 1850 Tchébychev établit la liaison de la fonction $\pi(x)$ avec la relation $\frac{x}{\log x}$. Il démontra le théorème suivant: *Il existe des constantes positives a et b, $a < b$, telles que pour tous x suffisamment grands on ait*

$$(1) \qquad a \cdot \frac{x}{\log x} < \pi(x) < b \frac{x}{\log x}.$$

On fournit plus bas la démonstration du théorème: *pour tous $x \geqslant 2$ on a les inégalités*

$$(2) \qquad \log 2 \cdot \frac{x}{\log x} - 2 < \pi(x) < 4 \log 2 \frac{x}{\log x} + \log_2 x \; .$$

Sur la base des inégalités (2) on est en mesure d'obtenir les constantes a et b des inégalités (1).

Pour démontrer les inégalités (2) on introduit la fonction $T(x) = \log [x]!$ et on établit les majorant et minorant de la fonction $T(x) - 2T\left(\frac{x}{2}\right)$.

Fonctions $T(x)$ et $\Lambda(x)$. Le symbole $\Lambda(x)$ désigne la fonction dont la valeur est $\log p$, si n est un nombre premier ou un exposant positif du nombre premier p, dans les autres cas sa valeur est zéro

$$\Lambda(n) = \begin{cases} \log p \text{ si } n = p^m \text{ pour tout nombre naturel } m > 0, \\ 0 \text{ si } n \neq p^m. \end{cases}$$

Plus loin on se servira de la propriété suivante de cette fonction:

$$(1) \qquad \sum_{d \mid n} \Lambda(d) = \log n.$$

Soit $n = \prod_{p \mid n} p^{e_p}$ la décomposition canonique du nombre naturel n. On voit sans peine que

$$\sum_{d \mid n} \Lambda(d) = \sum_{p^\alpha \mid n} \log p = \sum_{p \mid n} e_p \log p = \log n,$$

où p^α parcourt toutes les puissances des nombres premiers inclus dans n.

Le symbole $T(x)$ désigne la fonction qui pour tout nombre réel $x \geqslant 0$ prend la valeur $\log [x]!$, c'est-à-dire

$$T(x) = \log [x]! = \sum_{n \leqslant x} \log n,$$

où $[x]$ est la partie entière du nombre x.

En sommant (1) en tous les entiers positifs $n \leqslant x$, il vient

$$\sum_{m \leqslant x} \Lambda(m) \left[\frac{x}{m} \right] = \sum_{n \leqslant x} \log n = \log [x]! = T(x).$$

On a ainsi démontré la proposition suivante.

Proposition 5.1. *Pour tout nombre réel $x \geqslant 1$*

$$(1) \quad T(x) = \sum_{m \leqslant x} \Lambda(m) \left[\frac{x}{m} \right].$$

Inégalités imposées à la fonction $T(x)$. Par définition de la fonction $T(x)$,

$$(1) \quad T(n) = \log n!,$$

pour tout x réel positif

$$(2) \quad T(x) = \log [x]!$$

En raison de (1), on a

$$(3) \quad T(2n) - 2T(n) = \log \frac{(2n)!}{(n!)^2} = \log C_{2n}^n.$$

Démontrons que pour tout nombre naturel $n \geqslant 2$ sont satisfaites les inégalités

$$(4) \quad \frac{4^n}{2n} < C_{2n}^n < 4^n.$$

On voit sans peine que $C_{2n}^n < (1+1)^{2n} = 4^n$. Les calculs qui suivent démontrent la seconde inégalité:

$$C_{2n}^n = \frac{2n(2n-1)(2n-2)\ldots 2\cdot 1}{n^2(n-1)^2\ldots 1^2} =$$

$$= \frac{2n(2n-1)}{n^2} \cdot \frac{(2n-2)(2n-3)}{(n-1)^2} \cdots \frac{2\cdot 1}{1^2} =$$

$$= 4^n \left(1 - \frac{1}{2n}\right)\left(1 - \frac{1}{2(n-1)}\right) \cdots \left(1 - \frac{1}{2}\right) =$$

$$= 4^n \cdot \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdots \frac{2n-1}{2n} > 4^n \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdots \frac{2n-1}{2n} = \frac{4^n}{2n}.$$

A partir de (3), en vertu de (4), il s'ensuit pour $n \geqslant 2$ les inégalités

$$(5) \quad T(2n) - 2T(n) < \log 4^n = 2n \log 2,$$

$$(6) \quad T(2n) - 2T(n) > \log \frac{4^n}{2n} = 2n \log 2 - \log 2n.$$

Soit x un nombre réel quelconque supérieur ou égal à 2 et soit $2n$ le plus grand nombre pair ne dépassant pas x. Alors, de l'égalité (2)

dérive

(7) $T(x) - T(2n) \leqslant \log x.$

$T(x)$ étant une fonction non décroissante, il s'ensuit de (5) et (7)

(8) $$T(x) - 2T\left(\frac{x}{2}\right) < x \log 2 + \log x.$$

En vertu de (6),

$$T(x) - 2T\left(\frac{x}{2}\right) > (x-2) \log 2 - \log x.$$

De là, pour $x \geqslant 4$, on obtient l'inégalité

(9) $$T(x) - 2T\left(\frac{x}{2}\right) > x \log 2 - 2 \log x \qquad (x \geqslant 4).$$

Inégalités de Tchébychev. On a obtenu plus haut (voir inégalité (8)) l'inégalité

(1) $$T(x) - 2T\left(\frac{x}{2}\right) < x \log 2 + \log x$$

et on a démontré l'égalité

(2) $$T(x) = \sum_{m \leqslant x} \Lambda(m) \left[\frac{x}{m}\right].$$

Si $\frac{x}{2} < m \leqslant x$, alors $2m > x$. Aussi de l'égalité $\left[\frac{x}{m}\right] = 1$ s'ensuit-il que $\left[\frac{x}{2m}\right] = 0$. De là et à partir de (2), il vient:

(3) $$T(x) - 2T\left(\frac{x}{2}\right) = \sum_{m \leqslant x} \Lambda(m) \left(\left[\frac{x}{m}\right] - 2\left[\frac{x}{2m}\right]\right) \geqslant$$

$$\geqslant \sum_{\frac{x}{2} < m \leqslant x} \Lambda(m) \geqslant \sum_{\frac{x}{2} < p \leqslant x} \log p \geqslant \log\left(\frac{x}{2}\right)\left[\pi(x) - \pi\left(\frac{x}{2}\right)\right].$$

En vertu de (2) et (3), on a

(4) $$\left(\pi(x) - \pi\left(\frac{x}{2}\right)\right) \log \frac{x}{2} < x \log 2 + \log x.$$

On déduit de cette inégalité en substituant successivement à x $\frac{x}{2}$, $\frac{x}{4}$, $\frac{x}{8}$, . . . une série d'inégalités:

(4′) $$\left(\pi\left(\frac{x}{2}\right) - \pi\left(\frac{x}{4}\right)\right) \log \frac{x}{4} < \frac{x}{2} \log 2 + \log \frac{x}{2},$$

(4″) $$\left(\pi\left(\frac{x}{4}\right) - \pi\left(\frac{x}{8}\right)\right) \log \frac{x}{8} < \frac{x}{4} \log 2 + \log \frac{x}{4}.$$

. . . .

En sommant les premiers membres des inégalités (4), (4'), (4"), . . ., il vient

$$\pi(x)\log\frac{x}{2}-\pi\left(\frac{x}{2}\right)\left(\log\frac{x}{2}-\log\frac{x}{4}\right)-$$
$$-\pi\left(\frac{x}{4}\right)\left(\log\frac{x}{4}-\log\frac{x}{8}\right)-\ldots=$$
$$=\pi(x)\log x-\left(\pi(x)+\pi\left(\frac{x}{2}\right)+\pi\left(\frac{x}{4}\right)+\ldots\right)\log 2>$$
$$>\pi(x)\log x-\left(x+\frac{x}{2}+\frac{x}{4}+\ldots\right)\log 2=$$
$$=\pi(x)\log x-2x\log 2.$$

La somme des seconds membres des inégalités (4), (4'), (4"), . . . sera inférieure à $2x\log 2+\log x\cdot\log_2 x$, vu que le nombre d'inégalités ne dépasse pas $\log_2 x$. On aboutit ainsi à l'inégalité

$$\pi(x)\log x-2x\log 2<2x\log 2+\log x\cdot\log_2 x,$$

d'où

$$\pi(x)<4\log 2\frac{x}{\log x}+\log_2 x.$$

En outre, l'inégalité obtenue a lieu pour tout $x\geqslant 2$.

On a démontré plus haut l'inégalité

$$T(x)=2T\left(\frac{x}{2}\right)>x\log 2-2\log x.$$

De plus, vu que $T(x)-2T\left(\frac{x}{2}\right)=\sum\limits_{m\leqslant x}\Lambda(m)\left(\left[\frac{x}{m}\right]-\left[\frac{x}{2m}\right]\right)$, on a

$$T(x)-2T\left(\frac{x}{2}\right)\leqslant\sum_{m\leqslant x}\Lambda(m)=\sum_{p\leqslant x}\left[\frac{\log x}{\log p}\right]\log p\leqslant$$
$$\leqslant\sum_{p\leqslant x}\frac{\log x}{\log p}\log p\leqslant\pi(x)\log x$$

Ainsi, $x\log 2-2\log x<\pi(x)\log x$. Par conséquent, pour tout $x\geqslant 2$

$$\log 2\frac{x}{\log x}-2<\pi(x),$$

c'est-à-dire qu'on a obtenu la borne inférieure de la forme cherchée pour $\pi(x)$.

On a ainsi démontré le théorème suivant.

THÉORÈME 5.2. *Pour tous $x\geqslant 2$ on a:*

$$\log 2\frac{x}{\log x}-2<\pi(x)<4\log 2\frac{x}{\log x}+\log_2(x).$$

En 1850 Tchébychev a démontré des inégalités plus strictes. Il a démontré que pour des x suffisamment grands sont satisfaites les inégalités

$$(0{,}92\ldots)\frac{x}{\log x} < \pi(x) \leqslant (1{,}105\ldots)\frac{x}{\log x}.$$

En démontrant ces inégalités Tchébychev au lieu de $T(x)-2T\left(\frac{x}{2}\right)$ s'est servi d'une expression plus compliquée:

$$T(x)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right)+T\left(\frac{x}{30}\right).$$

En 1851 Tchébychev a émis l'hypothèse sur la dépendance entre $\pi(x)$ et $\frac{x}{\log x}$;

$$\underline{\lim}\frac{\pi(x)}{x/\log x} \leqslant 1 \leqslant \overline{\lim}\frac{\pi(x)}{x/\log x},$$

de sorte que si la limite du rapport $\frac{\pi(x)}{x/\log x}$ existe, elle est égale à 1.

Le résultat fondamental de la théorie des nombres est la loi asymptotique de la distribution des nombres premiers démontrée pour la première fois en 1896 par Hadamard et La Vallée-Poussin. Cette loi stipule que *le rapport* $\pi(x)$: $\frac{x}{\log x}$ *tend vers* 1 *quand* x *croît indéfiniment*, c'est-à-dire

$$\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=1.$$

Nombres premiers des progressions arithmétiques. Etudions trois théorèmes (5.3-5.5) constituant des cas particuliers d'un théorème plus général — le théorème de Dirichlet.

THÉORÈME 5.3. *La suite arithmétique* $4n+3$ $(n=0, 1, \ldots)$ *contient une infinité de nombres premiers.*

Démonstration. Considérons le nombre M défini par l'égalité $M=4n!-1$, où n est un entier positif. M est un nombre de la forme $4k+3$, il ne peut être composé que de facteurs premiers de la forme $4k+1$, car le produit des nombres de la forme $4k+1$ est un nombre de forme identique:

$$(4k+1)(4k_1+1)=4(4kk_1+k+k_1)+1.$$

Par suite, le nombre M possède au moins un facteur premier de la forme $4k+3$ supérieur à n. Ainsi, pour chaque nombre naturel n il existe un nombre premier supérieur à n et ayant la forme $4k+3$. □

THÉORÈME 5.4. *La suite arithmétique* $6n+5$ $(n=0, 1, 2, \ldots)$ *contient une infinité de nombres premiers.*

Démonstration. Ce théorème se démontre de façon analogue au précédent. Considérons le nombre M défini par l'égalité

$M = 6n! - 1$, où n est un entier positif quelconque; M est un nombre de la forme $6k + 5$. Le nombre M ne peut être uniquement composé de facteurs premiers de la forme $6k + 1$, car le produit des nombres de la forme $6k + 1$ est un nombre de forme identique:

$$(6k + 1)(6k_1 + 1) = 6(6kk_1 + k + k_1) + 1.$$

Par suite, le nombre M possède au moins un facteur premier supérieur à n et ayant la forme $6k + 5$. □

THÉORÈME 5.5. *La suite arithmétique*

$$4n + 1 \qquad (n = 0, 1, 2, \ldots)$$

contient une infinité de nombres premiers.

Démonstration. Soit n tout nombre naturel supérieur à l'unité. Alors, $(n!)^2 + 1$, étant un nombre impair, est plus grand que l'unité et possède un facteur premier impair p; p est donc de la forme $4k + 1$ ou $4k + 3$. Posons que $p = 4k + 3$. Vu que pour des a naturels et des m impairs

$$a + 1 \mid (a^m + 1), \text{ on a } (n!)^2 + 1 \mid (n!)^{2(2k+1)} + 1.$$

Comme $2(2k + 1) = 4k + 2 = p - 1$ et

$$p \mid (n!)^2 + 1, \text{ on a } p \mid (n!)^{p-1} + 1.$$

Par conséquent,

$$(1) \quad p \mid (n!)^p + n!$$

D'autre part, selon le théorème de Fermat

$$(2) \quad p \mid (n!)^p - n!$$

Il s'ensuit de (1) et (2) que $p \mid 2(n!)$, ce qui est impossible, vu que p est un nombre premier impair supérieur à n. Par conséquent, p doit être un nombre de la forme $4k + 1$. On a démontré que pour tout nombre naturel n il existe un nombre premier supérieur à n et ayant la forme $4k + 1$. □

Les théorèmes démontrés plus haut sont des cas particuliers du théorème de Dirichlet sur les progressions arithmétiques: *toute suite arithmétique* $a + km$ ($k = 0, 1, 2, \ldots$), *où* $(a, m) = 1$ *contient une infinité de nombres premiers.*

Exercices

1. Montrer que le polynôme $x^2 + x + 41$ prend pour la suite des nombres $x = 0, 1, 2, \ldots, 39$ des valeurs qui sont des nombres premiers distincts.

2. Soit f un polynôme en x de puissance positive à coefficients entiers. Démontrer que pour le nombre infini des x naturels le nombre $f(x)$ est un nombre composé.

3. En s'appuyant sur le théorème de Dirichlet sur les progressions arithmétiques démontrer que pour tout nombre naturel m il existe un nombre premier dont l'image graphique (dans le système de numération décimale ou tout autre système de numération à base naturelle $q > 1$) contient au moins m zéros.

CHAPITRE XII

THÉORIE DES CONGRUENCES AVEC APPLICATIONS ARITHMÉTIQUES

§ 1. Congruences et leurs propriétés

Congruences dans un anneau des entiers. Soient $\mathbf{Z}$ un anneau des entiers, m un entier fixé et $m\mathbf{Z}$ l'ensemble de tous les entiers multiples de m.

DEFINITION. Deux entiers a et b sont dits *congrus modulo m* si m divise $a - b$.

Si a et b sont congrus modulo m, on le note ainsi:

(1) $a \equiv b \pmod{m}$.

La congruence modulo m possède les propriétés de réflexivité, de symétrie et de transitivité, c'est-à-dire est une relation d'équivalence. Par conséquent, la congruence induit la partition de l'ensemble $\mathbf{Z}$ des entiers en classes d'équivalence qu'on appelle *classes résiduelles modulo m*.

Notons que la congruence modulo m coïncide avec la congruence modulo $(-m)$. La congruence modulo 0 coïncide avec la relation d'égalité. Deux entiers quelconques sont congrus modulo 1.

Comme la congruence modulo m est une relation d'équivalence sur l'ensemble $\mathbf{Z}$, les classes d'équivalence, c'est-à-dire les classes résiduelles modulo m, possèdent les propriétés suivantes:

PROPRIÉTÉ 1.1. *Toutes deux classes résiduelles modulo m ou bien coïncident, ou bien sont disjointes. La réunion de toutes les classes résiduelles modulo m coïncide avec l'ensemble* $\mathbf{Z}$ *de tous les entiers.*

PROPRIÉTÉ 1.2. *Soient A et B des classes résiduelles modulo m,* $a \in A$ *et* $b \in B$. *Les classes A et B suivant un sous-groupe coïncident si et seulement si* $a \equiv b \pmod{m}$.

PROPRIÉTÉ 1.3. *Si A est une classe résiduelle modulo m et a un élément quelconque de A, alors* $A = a + m\mathbf{Z}$, *c'est-à-dire* $A = \{a + mk \mid k \in \mathbf{Z}\}$.

PROPOSITION 1.1. *Les nombres a et b sont congrus modulo m* $(m \neq 0)$ *si et seulement si après division par m ils donnent des restes identiques.*

Démonstration. Supposons qu'après division avec reste des nombres a et b par m on aboutit aux quotients q et q_1 et aux restes r et r_1,

$$a = qm + r,\ 0 \leqslant r < m;\ b = q_1m + r_1,\ 0 \leqslant r_1 < m.$$

Posons que $r > r_1$. En soustrayant de la première égalité la deuxième, il vient

(1) $a - b = (q - q_1)\, m + (r - r_1), \quad 0 \leqslant r - r_1 < m.$

Si $a \equiv b \pmod m$, alors, par définition de la congruence, $a - b$ est divisible par m, donc $r - r_1 = 0$ et $r = r_1$. D'autre part, si $r = r_1$, alors, en vertu de (1), $a - b$ est divisible par m, c'est-à-dire $a \equiv b \pmod m$. □

Propriétés élémentaires des congruences. Plusieurs propriétés des congruences sont analogues aux propriétés des égalités.

PROPRIÉTÉ 1.4. *Les congruences peuvent être additionnées et soustraites membre à membre, c'est-à-dire si* $a \equiv b \pmod m$, $c \equiv d \pmod m$, *alors* $a + c \equiv b + d \pmod m$.

Démonstration. Par hypothèse, $m \mid (a - b)$ et $m \mid (c - d)$. Donc, $m \mid (a - b) \pm (c - d)$, $m \mid (a + c) - (b + d)$ et $m \mid (a - c) - (b - d)$. □

PROPRIÉTÉ 1.5. *Les congruences peuvent être multipliées membre à membre, c'est-à-dire si* $a \equiv b \pmod m$, $c \equiv d \pmod m$, *alors* $ac \equiv bd \pmod m$.

En particulier, les deux parties de la congruence peuvent être multipliées par le même entier.

Démonstration. Par hypothèse, $a - b \in m\mathbf{Z}$ et $c - d \in m\mathbf{Z}$. Donc, $ac - bd = (ac - bc) + (bc - bd) = (a - b)\, c + b\, (c - d) \in m\mathbf{Z}$, c'est-à-dire $ac \equiv bd \pmod m$. □

PROPRIÉTÉ 1.6. *Les deux parties de la congruence peuvent être divisées par leur facteur commun si ce dernier et le module sont premiers entre eux.*

Démonstration. Si $ca \equiv cb \pmod m$, c'est-à-dire $m \mid c\,(a - b)$ et les nombres c et m sont premiers entre eux, alors m divise $a - b$. Par conséquent, $a \equiv b \pmod m$. □

PROPRIÉTÉ 1.7. *Les deux parties de la congruence et le module peuvent être divisés par leur diviseur commun.*

Démonstration. Si $ka \equiv kb \pmod{mk}$, alors $k\,(a - b)$ se divise par km. Par conséquent, $a - b$ est divisible par m, c'est-à-pire $a \equiv b \pmod m$. □

PROPRIÉTÉ 1.8. *Soit m_1 un diviseur quelconque de m. Si* $a \equiv b \pmod m$, *alors* $a \equiv b \pmod{m_1}$.

Démonstration. Si $a \equiv b \pmod m$, alors $a - b$ est divisible par m. Or, m_1 est un diviseur de m, donc $a - b$ se divise par m_1, c'est-à-dire $a \equiv b \pmod{m_1}$. □

Exercices

1. Montrer que tout nombre naturel transcrit en numération décimale est congru modulo 9 et modulo 3 avec la somme de ses chiffres.
2. Établir la règle de vérification par 9 des opérations arithmétiques.

3. Chercher les caractères de divisibilité par 9 et 19 des nombres du système de numération décimale.

4. Chercher les caractères de divisibilité par 7 et 13 des nombres du système de numération décimale.

5. Chercher les caractères de divisibilité par 2, 3, 4, 5, 7, 9 dans le système de numération octale.

6. Chercher les caractères de divisibilité par 2, 3, 4, 5, 6, 7, 8, 9, 11, 13 dans le système de numération dodécanaire.

7. Démontrer que si $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$ et m, n des nombres premiers entre eux, on a $a \equiv b \pmod{mn}$.

8. Soit d le plus grand commun diviseur des entiers m et n. Montrer que si $a \equiv b \pmod{m}$ et $a \equiv b \pmod{n}$, alors $a \equiv b \left(\bmod \frac{mn}{d}\right)$.

§ 2. Système complet de résidus

Système complet de résidus. Selon la propriété 1.1 chaque classe résiduelle modulo m est définie de façon univoque par tout nombre a appartenant à cette classe; cette classe est un ensemble de tous les nombres de la forme $a + km$, c'est-à-dire est l'ensemble

$$\{a + km \mid k \in \mathbf{Z}\} = a + m\mathbf{Z}.$$

La classe résiduelle modulo m comprenant le nombre a, c'est-à-dire la collection de tous les entiers b tels que $b \equiv a \pmod{m}$ est notée tout simplement $a \bmod m$:

$$a \bmod m = \{a + km \mid k \in \mathbf{Z}\}.$$

Tout nombre appartenant à la classe résiduelle $a \bmod m$ est appelé *représentant de cette classe*.

DÉFINITION. On appelle *système complet des résidus modulo m* la collection de m entiers contenant strictement un représentant de chaque classe résiduelle modulo m.

Chaque classe résiduelle modulo m contient strictement un des nombres de la collection de tous les restes possibles de la division par m, à savoir $0, 1, 2, \ldots, m - 1$.

DÉFINITION. La collection des nombres $0, 1, 2, \ldots, m - 1$ est appelée *système des plus petits résidus non négatifs modulo m*.

Partout plus loin la notation $(a, m) = 1$ signifiera que les nombres a et m sont premiers entre eux.

PROPOSITION 2.1. *Toute collection de m nombres ($m > 1$) non congrus deux à deux modulo m constituent un système complet des résidus modulo m.*

D é m o n s t r a t i o n. Soit M la collection de m nombres non congrus deux à deux modulo m. Alors les nombres appartiennent à des classes résiduelles différentes. En outre, M comprend m nombres. Par conséquent, l'ensemble M contient un représentant de chaque classe résiduelle modulo m. □

PROPOSITION 2.2. *Soient a et b des entiers et $(a, m) = 1$. Si x parcourt le système complet des résidus modulo m, alors $ax + b$ parcourt aussi le système complet des résidus modulo m.*

Démonstration. Soit M le système complet des résidus. Alors, l'ensemble $M_1 = \{ax + b \mid x \in M\}$ contient, comme M, m éléments. Tous deux nombres $ax_1 + b$ et $ax_2 + b$ de M sont non congrus si $x_1 \not\equiv x_2 \pmod m$. Donc, l'ensemble M_1 est un système complet des résidus modulo m. □

Groupe additif des classes de résidus. Désignons par $\mathbf{Z}/m\mathbf{Z}$ l'ensemble de toutes les classes résiduelles modulo m:

$$\mathbf{Z}/m\mathbf{Z} = \{0 \bmod m,\ 1 \bmod m,\ \ldots,\ (m-1) \bmod m\}.$$

Définissons les opérations $+$, $-$ sur l'ensemble des classes résiduelles de la façon suivante:

$$a \bmod m + b \bmod m = (a + b) \bmod m,$$

$$-(a \bmod m) = (-a) \bmod m.$$

Selon les propriétés 1.4 et 1.5 des congruences, la congruence appliquée à l'ensemble $\mathbf{Z}$ est une congruence par rapport à l'opération d'addition dans $\mathbf{Z}$ et l'opération de passage à l'élément opposé. Ainsi, à deux classes quelconques $a \bmod m$ et $b \bmod m$ indépendamment du choix des représentants a et b en leur sein s'associe de façon univoque la classe $(a + b) \bmod m$ qui est leur somme. De façon analogue, la classe $-(a \bmod m)$ est indépendante du choix du représentant a. Vu que l'addition des entiers est commutative et associative, l'addition des classes des résidus est aussi commutative et associative, c'est-à-dire pour tous $a, b, c \in \mathbf{Z}$

$$a \bmod m + b \bmod m = b \bmod m + a \bmod m,$$

$$(a \bmod m + b \bmod m) + c \bmod m = a \bmod m + (b \bmod m + c \bmod m).$$

La classe des résidus $0 \bmod m$ est un élément neutre par rapport à l'addition, c'est-à-dire pour toute classe des résidus $a \bmod m$:

$$a \bmod m + 0 \bmod m = a \bmod m.$$

Ensuite, les classes $a \bmod m$ et $(-a) \bmod m$ sont mutuellement opposées, c'est-à-dire

$$a \bmod m + (-a) \bmod m = 0 \bmod m.$$

On aboutit donc au théorème suivant.

THÉORÈME 2.3. *L'algèbre $\langle \mathbf{Z}/m\mathbf{Z}, +, - \rangle$ constitue un groupe. Ce groupe est un groupe quotient du groupe $\mathfrak{Z}$ suivant le sous-groupe $m\mathfrak{Z}$.*

DÉFINITION. Le groupe $\langle \mathbf{Z}/m\mathbf{Z}, +, - \rangle$ est appelé *groupe additif des classes résiduelles modulo m.*

Anneau des classes résiduelles. Sur l'ensemble des classes résiduelles modulo m définissons la multiplication de la façon suivante:

$$(a \bmod m)\cdot(b \bmod m) = ab \bmod m.$$

Selon la propriété 1.5 des congruences, la congruence modulo m sur **Z** est une congruence par rapport à l'opération de multiplication sur **Z**. Ainsi, à chaque deux classes résiduelles $a \bmod m$ et $b \bmod m$, indépendamment du choix en leur sein des représentants a, b, s'associe de façon univoque la classe résiduelle $ab \bmod m$ qui est leur produit. Vu que les opérations d'addition et de multiplication des classes résiduelles se réduisent à des opérations appropriées sur les nombres de ces classes résiduelles, ces opérations respectent les lois de l'addition et de la multiplication, en particulier, les lois de commutativité, d'associativité et de distributivité

$$(a \bmod m)\,(b \bmod m) = (b \bmod m)\,(a \bmod m),$$

$$(a \bmod m)\,[(b \bmod m)\,(c \bmod m)] = [(a \bmod m)\,(b \bmod m)]\,(c \bmod m),$$

$$(a \bmod m)\,[(b \bmod m) + (c \bmod m)] = (a \bmod m)\,(b \bmod m) + (a \bmod m)\,(c \bmod m).$$

En outre, la classe résiduelle $1 \bmod m$ est un élément neutre par rapport à la multiplication:

$$(a \bmod m)\,(1 \bmod m) = a \bmod m.$$

Le théorème suivant est par suite vérifié.

THÉORÈME 2.4. *L'algèbre* $\langle \mathbf{Z}/m\mathbf{Z}, +, -, \cdot, 1 \bmod m\rangle$ *est un anneau commutatif (abélien).*

DÉFINITION. L'anneau $\langle \mathbf{Z}/m\mathbf{Z}, +, -, \cdot, 1 \bmod m\rangle$ est appelé *anneau des classes résiduelles modulo m.*

Exercices

1. Chercher le système complet des résidus et le système des absolument plus petits résidus modulo 30.
2. Chercher le système complet des absolument plus petits résidus modulo 19.
3. Les puissances 2^0, 2^1, 2^2, ..., 2^{10} avec le nombre 0 forment-elles un système complet des résidus modulo 11?
4. En portant dans l'expression $3x + 7y$ les valeurs de $x = 0, 1, 2, 3, 4, 5, 6$ et de $y = 0, 1, 2$ vérifier qu'on obtient finalement un système complet des résidus modulo 21.

§ 3. Système réduit des résidus

Système réduit des résidus. Soit n un nombre positif quelconque. Notons $\varphi(n)$ le nombre d'entiers positifs ne dépassant pas n et premiers avec n. Le plus grand commun diviseur des entiers a, b qui est un nombre naturel sera noté (a, b).

PROPOSITION 3.1. *Tous les nombres de la classe résiduelle fixée* a mod m *possèdent avec* m *un même plus grand commun diviseur, égal à* (a, m).

Démonstration. Si b est un nombre quelconque de la classe résiduelle a mod m, alors $b = mq + a$, où q est un certain entier. De là, en vertu de la proposition 11.3.1, il s'ensuit que $(b, m) = (a, m)$. □

Par conséquent, (a, m) ne dépend que de la classe résiduelle a mod m et est indépendant du choix du représentant a dans cette classe. En particulier, si $(a, m) = 1$, la classe a mod m est appelée *classe résiduelle constituant un élément premier avec le module m.*

PROPOSITION 3.2. *Le nombre des classes résiduelles, formant avec m des éléments premiers, vaut* $\varphi(m)$.

Démonstration. A partir du système complet des résidus modulo m

$1, 2, \ldots, m$

dégageons le système de tous les résidus premiers avec m:

$a_1, a_2, \ldots, a_{\varphi(m)}$.

En vertu de la proposition 3.1, les classes résiduelles

(1) $a_1 \bmod m, a_2 \bmod m, \ldots, a_{\varphi(m)} \bmod m$

sont des éléments premiers avec le module m. Toute autre classe n'entrant pas dans (1) n'est pas première avec le module m, car elle contient un élément de l'ensemble $\{1, 2, \ldots, m\} \setminus \{a_1, a_2, \ldots, a_{\varphi(m)}\}$. Les classes figurant dans le système (1) sont distinctes. Par conséquent, le nombre des classes, formant avec m des éléments premiers, vaut $\varphi(m)$. □

DÉFINITION. On appelle *système réduit des résidus modulo m* la collection d'entiers contenant un représentant de chaque classe résiduelle, premier avec m.

PROPOSITION 3.3. *Toute collection* $\varphi(m)$ *des nombres,* $m > 1$, *premiers avec m et deux à deux non congrus modulo m est un système réduit des résidus modulo m.*

Démonstration. Soit M une collection $\varphi(m)$ de nombres premiers avec m et non congrus deux à deux modulo m. Ces nombres appartiennent alors à des classes résiduelles différentes. Donc, l'ensemble M renferme un représentant de chaque classe résiduelle, premier avec le module m. Par conséquent, M est un système réduit de résidus modulo m. □

PROPOSITION 3.4. *Soient a un entier premier avec m et* $b_1, b_2, \ldots, b_{\varphi(m)}$ *un système réduit des résidus modulo m. Alors, la collection* $ab_1, ab_2, \ldots, ab_{\varphi(m)}$ *est aussi un système réduit des résidus modulo m.*

Démonstration. En raison de la proposition 3.3 il suffit de montrer que les nombres de la collection $ab_1, ab_2, \ldots, ab_{\varphi(m)}$ sont deux à deux non congrus modulo m. En effet, si $ab_l \equiv ab_k \times$

$\times$ (mod m) avec $i \neq k$, on a alors, selon la condition $(a, m) = 1$, $b_i \equiv b_k$ (mod m), ce qui est impossible vu que par hypothèse de la proposition b_i et b_k sont des éléments distincts du système réduit des résidus modulo m. □

Groupe multiplicatif des classes résiduelles, éléments premiers avec le module. Considérons le théorème dégageant une propriété fort importante des classes résiduelles, éléments premiers avec le module.

THÉORÈME 3.5. *L'ensemble des classes résiduelles modulo m formant des éléments premiers avec le module constituent par rapport à la multiplication un groupe abélien.*

D é m o n s t r a t i o n. Soit G_m l'ensemble de toutes les classes résiduelles modulo m éléments premiers avec m. Le produit de deux classes résiduelles quelconques modulo m éléments premiers avec le module constitue une classe résiduelle formant des éléments premiers avec le module et, par suite, l'ensemble G_m est fermé par rapport à la multiplication. Ensuite, l'opération de multiplication des classes est commutative et associative. La classe $\bar{1}$, $\bar{1} = 1$ mod m est l'élément neutre par rapport à la multiplication. Démontrons que pour toute classe $\bar{a} \in G_m$ il existe dans G_m une classe inverse. Soit

$$G_m = \{\bar{a}_1, \ldots, \bar{a}_{\varphi(m)}\},$$

c'est-à-dire que $a_1, a_2, \ldots, a_{\varphi(m)}$ est un système réduit des résidus modulo m. Alors, selon la proposition 3.4 $aa_1, aa_2, \ldots, aa_{\varphi(m)}$ est aussi un système réduit des résidus modulo m; il renferme donc un nombre congru avec 1. Soit $aa_k \equiv 1$ (mod m). Alors $\bar{a}\bar{a}_k = \bar{1}$, et, partant, $\bar{a}_k$ est une classe inverse de la classe $\bar{a}$ de G_m. Ainsi, le système $\langle G_m, \cdot, {}^{-1}\rangle$ est un groupe abélien. □

DÉFINITION. Le groupe $\mathcal{G}_m = \langle G_m, \cdot, {}^{-1}\rangle$ est dit *groupe multiplicatif des classes résiduelles modulo m*, formant avec le module des éléments premiers.

COROLLAIRE 3.6. *Si p est un nombre premier, alors l'ensemble des classes résiduelles non nulles est un groupe abélien par rapport à la multiplication.*

THÉORÈME 3.7. *Un anneau des classes résiduelles modulo m constitue un corps si et seulement si m est un nombre premier.*

D é m o n s t r a t i o n. Soit m un nombre premier. Alors, selon la corollaire 3.6, l'ensemble de toutes les classes résiduelles non nulles modulo m est un groupe par rapport à la multiplication. Aussi l'anneau des classes résiduelles modulo m est-il un corps.

Soit m un nombre composé. $m = ab$, $1 < a, b < m$. Dans ce cas (a mod m) (b mod m) = 0 mod m, de plus, par hypothèse.

$$a \bmod m \neq 0 \bmod m, \quad b \bmod m \neq 0 \bmod m.$$

Ainsi, l'anneau des classes résiduelles comporte des diviseurs de zéro et, partant, ne peut être un corps.

24—01762

Si $m = 1$, l'anneau des classes résiduelles modulo m est alors un anneau réduit à $\{0\}$. Si, par contre, $m = 0$, l'anneau des classes résiduelles modulo m, $\mathbb{Z}/(0)$, est isomorphe à l'anneau $\mathbb{Z}$ et, par suite, n'est pas un corps. □

DÉFINITION. Le nombre a est dit *inverse du nombre b modulo m* si $ab \equiv 1 \pmod{m}$. Les nombres a et b seront également appelés *mutuellement inverses modulo m.*

PROPOSITION 3.8. *Soient a un nombre premier avec le module m et P_{n-1} le numérateur de l'avant-dernière réduite du nombre $\frac{m}{a}$ $\left(\frac{m}{a} = \frac{P_n}{Q_n}\right)$. Alors, $a(-1)^{n-1} P_{n-1} \equiv 1 \pmod{m}$, c'est-à-dire que le nombre $(-1)^{n-1} P_{n-1}$ est l'inverse de l'élément a modulo m.*

Démonstration. Soient $\frac{P_{n-1}}{Q_{n-1}}$ et $\frac{P_n}{Q_n}$ les deux dernières réduites du nombre m/a. Alors $m = P_n$, $a = Q_n$ et, selon le corollaire 11.3.5,

$$\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^n}{Q_{n-1}Q_n}.$$

Par conséquent,

$$\frac{m}{a} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^n}{Q_{n-1}Q_n}, \quad Q_{n-1}m - aP_{n-1} = (-1)^n \text{ et}$$

$$a(-1)^{n-1} P_{n-1} \equiv 1 \pmod{m}. \ \square$$

Exemple. Cherchons le nombre inverse du nombre 79 modulo $m = 273$.

Décomposons le nombre $\frac{273}{79}$ en fraction continue, alors

$$\frac{273}{79} = |3;\ 2,\ 5,\ 7|.$$

Calculons les numérateurs des réduites du nombre $\frac{273}{79}$ suivant le schéma

k		1	2	3	4
q_k		3	2	5	7
p_k	1	3	7	38	273

$P_3 = 38$ est le numérateur de l'avant-dernière réduite du nombre 273/79. Donc, le nombre $(-1)^3 P_3 = -38$ est l'inverse du nombre 79, c'est-à-dire $79(-38) \equiv 1 \pmod{273}$.

Fonction d'Euler. Le nombre d'entiers positifs ne dépassant pas n et premiers avec lui est noté $\varphi(n)$; la fonction numérique φ définie sur l'ensemble de tous les entiers positifs est nommée *fonction*

d'Euler (ou *indicateur d'Euler*). On constate sans peine que $\varphi(n)$ est égal au nombre des entiers non négatifs inférieurs à n et premiers avec lui.

Exemple: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(6) = 2$, $\varphi(5) = 4$, $\varphi(12) = 4$.

La fonction numérique f est dite *multiplicative* si pour des entiers positifs a et b premiers entre eux, on a l'égalité $f(ab) = f(a) f(b)$.

THÉORÈME 3.9. *La fonction d'Euler φ est multiplicative.*

Démonstration. Soient a et b des entiers positifs premiers entre eux. Considérons l'ensemble M de tous les entiers non négatifs inférieurs à ab. Selon le théorème de la division avec reste, chaque nombre de M peut se représenter de façon unique sous forme de $bq + r$, où $r \in \{0, 1, \ldots, b-1\}$, $q \in \{0, 1, \ldots, a-1\}$. Le nombre $bq + r$ est premier avec a si et seulement si $(b, r) = 1$. Il existe $\varphi(b)$ de tels r. Soit r_1 l'un d'eux. Alors, selon la proposition 2.2, les nombres $r_1, b + r_1, 2b + r_1, \ldots, b(a-1) + r_1$ forment un système complet des résidus modulo a. Il existe donc parmi ces nombres exactement $\varphi(a)$ nombres premiers avec a. Ainsi, à chaque nombre r_1 premier avec b sont associés exactement $\varphi(a)$ nombres de la forme $bq + r_1$ premiers avec a et, partant, avec ab. Aussi le nombre de nombres appartenant à M et premiers avec ab est-il égal à $\varphi(a)\varphi(b)$, c'est-à-dire $\varphi(ab) = \varphi(a)\varphi(b)$.

THÉORÈME 3.10. *Si $n = \prod_{p \mid n} p^{\alpha_p}$ est une décomposition canonique, du nombre naturel n, alors*

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right). \tag{1}$$

Démonstration. Vu que la fonction φ est multiplicative, pour le calcul de $\varphi(n)$ il suffit d'être en mesure de calculer cette fonction pour une puissance du nombre premier p. Le nombre des entiers non négatifs inférieurs à p^α et non premiers avec p^α vaut $p^{\alpha-1}$, car seuls les nombres kp, $0 \leqslant k < p^{\alpha-1}$ ne sont pas premiers avec p^α. Aussi le nombre de nombres inférieurs à p^α et premiers avec p^α vaut-il $p^\alpha - p^{\alpha-1}$, c'est-à-dire

$$\varphi(p^\alpha) = p^\alpha \left(1 - \frac{1}{p}\right). \tag{2}$$

Vu que $n = \prod_{p \mid n} p^{\alpha_p}$ et la fonction φ est multiplicative, on a

$$\varphi(n) = \prod_{p \mid n} \varphi(p^{\alpha_p}). \tag{3}$$

De (2) et (3) il s'ensuit que

$$\varphi(n)=\prod_{p\mid n} p^{\alpha_p}\left(1-\frac{1}{p}\right)=\prod_{p\mid n} p^{\alpha_p}\prod_{p\mid n}\left(1-\frac{1}{p}\right)=$$
$$=n\prod_{p\mid n}\left(1-\frac{1}{p}\right),$$

et, par suite, la formule (1) est vérifiée. □

Exemple: $\varphi(30)=30\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=$
$$=30\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}=8.$$

Théorème 3.11. *La somme des nombres $\varphi(d)$ suivant tous les diviseurs naturels d du nombre n vaut n, c'est-à-dire* $\sum_{d\mid n}\varphi(d)=n$.

Démonstration. Si $n=\prod_i p_i^{\alpha_i}$ est une décomposition canonique de n, alors

$$\sum_{d\mid n}\varphi(d)=\prod_i(1+\varphi(p_i)+\varphi(p_i^2)+\ldots+\varphi(p_i^{\alpha_i})),$$

puisqu'en ouvrant les parenthèses, on obtient la somme de toutes les valeurs de $\varphi(d)$. Ensuite,

$$\sum_{d\mid n}\varphi(d)=\prod_i(1+(p_i-1)+(p_i^2-p_i)+\ldots+(p_i^{\alpha_i}-p_i^{\alpha_i-1})=$$
$$=\prod_i p_i^{\alpha_i}=n,\ \text{c'est-à-dire}\ \sum_{d\mid n}\varphi(d)=n.$$

Théorèmes d'Euler et de Fermat. En théorie des congruences un rôle important est joué par le théorème d'Euler.

Théorème d'Euler. *Si un entier a est un nombre premier avec m, alors*

(1) $a^{\varphi(m)}\equiv 1 \pmod m$.

Démonstration. Soit

(2) $a_1, a_2, \ldots, a_{\varphi(m)}$

un système réduit des résidus modulo m. Alors, selon la proposition 3.4,

(3) $aa_1, aa_2, \ldots, aa_{\varphi(m)}$

l'est également. Aussi le produit des nombres (3) est-il congru au produit des nombres (2), c'est-à-dire

(4) $a^{\varphi(m)}a_1a_2\ldots a_{\varphi(m)}\equiv a_1a_2\ldots a_{\varphi(m)} \pmod m$.

Le produit $a_1a_2 \ldots a_{\varphi(m)}$ est premier avec m. Aussi, selon la propriété 1.6, les deux parties de la congruence (4) se prêtent-elles à une division par ce produit et on a $a^{\varphi(m)} \equiv 1 \pmod m$. □

THÉORÈME de FERMAT. *Si un nombre entier a n'est pas divisible par le nombre premier p, alors* $a^{p-1} \equiv 1 \pmod p$.

Ce théorème est un cas particulier du théorème précédent au cas où $m = p$. On énonce souvent le théorème de Fermat de façon différente.

SECOND ÉNONCÉ DU THÉORÈME DE FERMAT. *Si p est premier et a un entier quelconque, alors* $a^p \equiv a \pmod p$.

Exercices

1. En partant de l'égalité $a^p = (1 + 1 + \ldots + 1)^p$, démontrer que pour tout a naturel et p premier la congruence $a^p \equiv a \pmod p$ est satisfaite.

2. Démontrer que le nombre des fractions réduites positives ayant pour dénominateurs l'un des nombres suivants: $1, 2, \ldots, n$ et ne dépassant pas l'unité vaut $\varphi(1) + \varphi(2) + \ldots + \varphi(n)$.

3. Démontrer que pour $n > 1$ la somme des résidus m modulo n se disposant dans l'intervalle $1 \leqslant m < n$ est égale à $\frac{1}{2} n\varphi(n)$.

4. Montrer sur des exemples que la congruence $a^m \equiv a \pmod m$, où m est premier, peut ne pas se vérifier pour un m composé.

5. Démontrer que si $a^{n-1} \equiv 1 \pmod n$ et $a^d \not\equiv 1$ pour tout diviseur positif d du nombre $(n - 1)$, alors n est premier.

6. Combien y a-t-il de nombres naturels inférieurs au nombre 234 000 000 et premiers avec lui?

§ 4. Congruences du premier degré. Congruences de degrés supérieurs suivant un module simple

Degré et nombre de solutions de la congruence. La congruence de la forme

$$(1) \qquad a_nx^n + \ldots + a_1x + a_0 \equiv 0 \pmod m,$$

où $a_1, \ldots, a_n$ sont des entiers, est appelée *congruence algébrique*. Le nombre n est dénommé *degré de la congruence* (1) si a_n n'est pas divisible par m.

Si le nombre a satisfait à la congruence (1), alors tout nombre b congru à a modulo m satisfait également à la congruence (1); ces deux solutions sont considérées comme identiques.

DÉFINITION. On appelle *nombre de solutions de la congruence modulo m* le nombre de solutions de cette congruence au sens d'un système complet quelconque des résidus modulo m.

Exemples. 1. La congruence $3x^2 - 7 \equiv 0 \pmod 4$ parmi les nombres 0, 1, 2, 3 du système complet des résidus modulo 4 est satisfaite pour deux nombres: $x = 1$ et $x = 3$. La congruence a donc deux solutions: $x \equiv 1 \pmod 4$ et $x \equiv 3 \pmod 4$.

2. A la congruence $x^2 \equiv 1 \pmod 8$, parmi les nombres 0, 1, 2, 3, 4, 5, 6, 7 du système complet des résidus modulo 8, satisfont quatre nombres: 1, 3, 5, 7. Aussi, la congruence a-t-elle quatre solutions:

$$x \equiv 1 \pmod 8, \quad x \equiv 3 \pmod 8, \quad x \equiv 5 \pmod 8, \quad x \equiv 7 \pmod 8.$$

Congruences du premier degré. Cherchons les conditions de résolubilité de la congruence du premier degré.

THÉORÈME 4.1. *Si $(a, m) = 1$, alors la congruence*

(1) $ax \equiv b \pmod m$

admet une et seulement une solution.

Démonstration. Par hypothèse le nombre a est premier avec m. Selon le théorème 3.5, il existe un entier a' inverse de a modulo m, c'est-à-dire $a'a \equiv 1 \pmod m$. Multiplions les deux membres de (1) par a', il vient

(2) $x \equiv a'b \pmod m$.

Par conséquent, la congruence (1) admet une solution au plus. D'autre part, (2) est une solution de la congruence (1), car

$$a\,(a'b) \equiv (aa')\,b \equiv b \pmod m.$$

Ainsi, la classe résiduelle $a'b \bmod m$ est l'unique solution de la congruence (1). □

THÉORÈME 4.2. *Soit $(a, m) = d$. La congruence*

(1) $ax \equiv b \pmod m$

est résoluble si et seulement si $d \mid b$. Si $d \mid b$, la congruence (1) *possède en guise de solutions exactement d classes résiduelles modulo m qui constituent une classe résiduelle commune modulo m/d.*

Démonstration. Soit $(a, m) = d > 1$. Si la congruence (1) a pour solution x_1, alors $ax_1 - b = km$, où k est un entier. Vu que $(a, m) = d$, il s'ensuit que d divise b.

Admettons maintenant que b est divisible par d et démontrons que la congruence (1) a d solutions. Soient $b = b_1d$, $a = a_1d$ et $m = m_1d$. La congruence (1) est équipotente à la congruence

(2) $a_1x \equiv b_1 \pmod{m_1}$.

Selon le théorème 4.1, la congruence (2) possède une solution unique $a_1'b_1 \bmod m_1$, où a_1' est un nombre inverse de a_1 modulo m_1. Soit $x_0 = a_1'b_1$. La classe résiduelle $x_0 \bmod m_1$ se sépare en d classes résiduelles modulo m suivantes:

(3) $x_0 \bmod m,\ (x_0 + m_1) \bmod m,\ (x_0 + 2m_1) \bmod m,\ \ldots$
$\ldots,\ (x_0 + (d-1)\,m_1) \bmod m.$

On constate sans peine que les classes résiduelles (3) sont des classes de module m distinct. Ainsi, la congruence (2) possède en guise de solutions des classes résiduelles (3), c'est-à-dire exactement d classes résiduelles modulo m constituant une classe résiduelle unique modulo m/d. □

Notons que la collection des solutions (3) de la congruence (1) est une classe du groupe additif $\mathcal{G}$ des classes résiduelles modulo m suivant le sous-groupe $\frac{m}{d}\cdot\mathcal{G}$. Réciproquement : toute classe suivant le sous-groupe $\frac{m}{d}\cdot\mathcal{G}$ du groupe $\mathcal{G}$ peut être prise pour un ensemble des solutions d'une certaine congruence linéaire modulo m.

Congruences de degrés supérieurs suivant un module simple. Passons au problème du nombre de solutions qu'admet une congruence de degré n suivant un module simple.

THÉORÈME 4.3. *La congruence*

(1) $a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \pmod p$

de degré n suivant un module simple p admet n solutions au plus.

D é m o n s t r a t i o n (s'effectue par récurrence sur n). Si $n = 0$, la congruence est de la forme $a_0 \equiv 0 \pmod p$, où $p \nmid a_0$; dans ce cas la congruence a zéro solutions. Supposons que la congruence (1) est de degré $n > 0$. Si la congruence admet des solutions, alors pour un certain entier x_1, on a

(2) $a_n x_1^n + \ldots + a_1 x_1 + a_0 \equiv 0 \pmod p$.

Soustrayons cette congruence de (1). Dans ce cas, la différence entre les termes de degré k est de la forme

$$a_k (x^k - x_1^k) = a_k (x - x_1)(x^{k-1} + x_1 x^{k-2} + \ldots + x_1^{k-1})$$

avec $k = 1, \ldots, n$; chaque différence contient un facteur linéaire $(x - x_1)$. Aussi peut-on finalement écrire la différence de la façon suivante :

(3) $(x - x_1)(b_{n-1} x^{n-1} + \ldots + b_0) \equiv 0 \pmod p$,

où $b_0, \ldots, b_{n-1}$ sont des entiers, $b_{n-1} = a_n$. Toute autre solution de la congruence (1), disons, x_2 sera la solution de la congruence

(4) $b_{n-1} x^{n-1} + \ldots + b_0 \equiv 0 \pmod p$.

En effet, vu que $x_2 \not\equiv x_1 \pmod p$ et le module p est simple, de la congruence

$$(x_2 - x_1)(b_{n-1} x_2^{n-1} + \ldots + b_0) \equiv 0 \pmod p$$

on tire que

$$b_{n-1} x^{n-1} + \ldots + b_0 \equiv 0 \pmod p.$$

Comme le degré de la congruence (4) vaut $n - 1$, suivant l'hypothèse de récurrence, la congruence (4) admet $n - 1$ solutions au plus. Donc, la congruence de départ (1) possède n solutions au plus. □

COROLLAIRE 4.4. *Si la congruence* $a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \pmod{p}$ *admet plus de n solutions, tous ses coefficients sont divisibles par p.*

PROPOSITION 4.5. *Si p est premier, la congruence* $x^{p-1} - 1 \equiv 0 \pmod{p}$ *admet exactement* $p - 1$ *solutions.*

Cette proposition découle directement du théorème de Fermat et tous nombres non divisibles par p satisfont à la congruence; ses solutions sont les nombres $1, 2, \ldots, p - 1$.

THEOREME de WILSON. *Si p est premier, alors*

(1) $$(p-1)! + 1 \equiv 0 \pmod{p}.$$

D é m o n s t r a t i o n. Si $p = 2$ le théorème est apparemment vrai. Soit $p > 2$. Considérons la congruence

(2) $$(x-1)(x-2)\ldots(x-(p-1)) - (x^{p-1} - 1) \equiv 0 \pmod{p}.$$

Son degré est inférieur à $p - 1$, mais cette congruence possède $p - 1$ solutions: $1, 2, \ldots, p - 1$. Aussi, selon le corollaire 4.4, tous les coefficients de la congruence (2) sont-ils divisibles par p. En particulier, le dernier coefficient égal à $(p - 1)! + 1$ est divisible par p. □

THEOREME 4.6. *Si p est premier et d est un diviseur naturel du nombre* $p - 1$, *la congruence*

(1) $$x^d - 1 \equiv 0 \pmod{p}$$

a alors exactement d solutions.

D é m o n s t r a t i o n. Soit d un diviseur quelconque de $p - 1$, $p - 1 = kd$. Alors la congruence

(2) $$x^{p-1} - 1 \equiv 0 \pmod{p}$$

peut être écrite sous la forme

(3) $$(x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \ldots + x^d + 1) \equiv 0 \pmod{p}.$$

Selon la proposition 4.5, la congruence (2) possède $p - 1$ solutions: $1, 2, \ldots, p - 1$. Chaque solution de la congruence (2) doit vérifier l'une des congruences:

(1) $$x^d - 1 \equiv 0 \pmod{p},$$

(4) $$x^{d(k-1)} + \ldots + x^d + 1 \equiv 0 \pmod{p}.$$

Selon le théorème 4.3, la congruence (4) admet $d(k-1) = p - 1 - d$ solutions au plus. Aussi, la congruence (1) doit-elle posséder au moins d solutions. Donc, en raison de la proposition 4.5, la congruence (3) a exactement d solutions. □

Exercices

1. Démontrer que si le nombre naturel $m > 1$, la congruence $1 \cdot 2 \cdot 3 \ldots$ $\ldots (m-1) \equiv -1 \pmod m$ est alors satisfaite si et seulement si m est premier.
2. Chercher les solutions de la congruence $ax \equiv 1 \pmod 7$ pour $a = 2, 3, 4, 5, 6$.
3. Chercher le nombre multiple de sept et fournissant le reste 1 après division par 2, 3, 4, 5, 6.
4. Démontrer que la congruence $x^2 + 1 \equiv 0 \pmod p$, pour $p = 4n + 1$ premier, est satisfaite pour le nombre $(2n)!$
5. Résoudre les congruences:

$x^2 \equiv -1 \pmod{65}$; $\qquad x^2 \equiv -2 \pmod{33}$.

§ 5. Racines primitives et indices

Ordre du nombre et de la classe résiduelle suivant un module. Soit a un nombre premier avec m. On appelle *ordre du nombre a modulo m* le plus petit entier positif d tel que $a^d \equiv 1 \pmod m$. Si $b \equiv a \pmod m$, il possède le même ordre modulo m que a. Ainsi, tous les éléments de la classe résiduelle a mod m sont d'ordre d; le nombre d est appelé *ordre de la classe résiduelle* a mod m et noté Θ (a mod m).

Proposition 5.1. *Si* Θ (a mod m) $= d$, *alors les nombres* $a, a^2, \ldots, a^d$ *sont non congrus deux à deux modulo* m.

Démonstration. Si $a^s \equiv a^k \pmod m$, où $k < s$, $k, s \in \{1, 2, \ldots, d\}$, alors $a^{s-k} \equiv 1 \pmod m$, ce qui est en contradiction avec l'hypothèse, car $0 < s - k < d$. □

Proposition 5.2. *Soient* Θ (a mod m) $= d$ *et* n *tout entier non négatif. La congruence* $a^n \equiv 1 \pmod m$ *est vérifiée si et seulement si* n *est divisible par* d.

Démonstration. Montrons d'abord qu'il s'ensuit à partir de $a^n \equiv 1 \pmod m$ que n est divisible par d. Selon le théorème de la division avec reste, il existe pour n et d des nombres naturels q et r tels que

$$(1) \qquad n = dq + r, \qquad 0 \leqslant r < d.$$

Montrons que $r = 0$. En raison de (1) et de la condition $a^d \equiv 1 \pmod m$, on a

$$a^n \equiv a^{dq}a^r \equiv (a^d)^q a^r \equiv a^r \equiv 1 \pmod m.$$

Vu que par hypothèse $a^r \not\equiv 1 \pmod m$, si $0 < r < d$, la congruence $a^r \equiv 1 \pmod m$ n'est possible que pour $r = 0$. Par conséquent, n est divisible par d. Supposons maintenant que n est divisible par d, $n = dk$ pour un certain k. Alors

$$a^n \equiv a^{dk} \equiv (a^d)^k \equiv 1 \pmod m, \text{ c'est-à-dire } a^n \equiv 1 \pmod m. \quad \square$$

Proposition 5.3. *Si* Θ (a mod m) $= d$, *alors* $\varphi(m)$ *est divisible par* d.

D é m o n s t r a t i o n. En vertu de la proposition 5.2, de $a^{\varphi(m)} \equiv 1 \pmod{m}$ et de la condition $\Theta(a \bmod m) = d$ il s'ensuit que $\varphi(m)$ est divisible par d. □

PROPOSITION 5.4. *Soit* $\Theta(a \bmod m) = d$. *La congruence* $a^s \equiv$ $\equiv a^k \pmod{m}$ *a lieu si et seulement si* $k \equiv s \pmod{d}$.

D é m o n s t r a t i o n. Si

(1) $a^k \equiv a^s \pmod{m}, \qquad k \geqslant s,$

alors,

(2) $a^{k-s} \equiv 1 \pmod{m}$

et, par suite, en vertu de la proposition 5.2, $k - s$ est divisible par d, c'est-à-dire

(3) $k \equiv s \pmod{d}$.

Réciproquement: de (3) s'ensuivent (2) et (1). □

PROPOSITION 5.5. *Soient* a, b *des nombres premiers avec* m. *Si les nombres* $\Theta(a \bmod m)$ *et* $\Theta(b \bmod m)$ *sont premiers entre eux, alors*

$$\Theta(ab \bmod m) = \Theta(a \bmod m) \cdot \Theta(b \bmod m).$$

D é m o n s t r a t i o n. Soient $\Theta(a) = d$, $\Theta(b) = e$ et $\Theta(ab) =$ $= f$. Démontrons que f est divisible par de. Vu que $b^e \equiv 1 \pmod{m}$, alors $a^e \equiv a^e b^e \equiv (ab)^e \pmod{m}$ et $a^{ef} \equiv (ab)^{ef} \equiv ((ab)^f)^e \equiv$ $\equiv 1 \pmod{m}$. A partir de $a^{ef} \equiv 1 \pmod{m}$, en vertu de la proposition 5.2, il s'ensuit que ef est divisible par d. Vu que par hypothèse $(d, e) = 1$, f est divisible par d. On obtient de même que f est divisible par e. Donc, f est divisible par de.

D'autre part, $(ab)^{de} \equiv (a^d)^e (b^e)^d \equiv 1 \pmod{m}$. Selon la proposition 5.2, il s'ensuit que de est divisible par f. Par conséquent, $f = de$. □

PROPOSITION 5.6. *Si* $\Theta(a \bmod m) = n$ *et* d *est un diviseur naturel du nombre* n, *alors* $\Theta(a^d \bmod m) = n/d$.

D é m o n s t r a t i o n. Soit $\Theta(a^d \bmod m) = f$. Par hypothèse, $a^n \equiv (a^d)^{n/d} \equiv 1 \pmod{m}$. Selon la proposition 5.2, il s'ensuit que n/d est divisible par f, c'est-à-dire $n/d = kf$, $n = kfd$ pour un certain nombre naturel k. Donc, $a^{fd} \equiv (a^d)^f \equiv 1 \pmod{m}$. On en déduit que fd est divisible par n. Donc, $k = 1$, $n = fd$ et $f = n/d$. □

PROPOSITION 5.7. *Si* $\Theta(a \bmod m) = n$ *et* $(k, n) = d$, *alors*

$$\Theta(a^k \bmod m) = n/d.$$

D é m o n s t r a t i o n. Soient $\Theta(a^k \bmod m) = f$, $k = k_1 d$, $n = n_1 d$. De l'hypothèse on déduit que

$$(a^k)^{n/d} \equiv (a^n)^{k/d} \equiv 1 \pmod{m}.$$

Par conséquent, le nombre $n/d = n_1$ est divisible par f. D'autre part, $(a^k)^f \equiv a^{kf} \equiv 1 \pmod{m}$. Selon la proposition 5.2, il s'ensuit

que kf est divisible par n. Donc, $k_1 f$ est divisible par n_1; vu que $(k_1, n_1) = 1$, f est donc divisible par n_1; par conséquent, $f = n_1 = n/d$. □

PROPOSITION 5.8. *Si* Θ $(a \bmod m) = n$ *et* $(k, n) = 1$, *alors* Θ $(a^k \bmod m) = n$.

Cette proposition découle directement de la précédente.

Racines primitives suivant un module simple. Pour décrire un groupe des résidus multiplicatif suivant un module simple il faut procéder à l'étude des nombres dont l'ordre est le plus grand suivant ce module.

THÉORÈME 5.9. *Soient p un nombre premier et d un diviseur naturel du nombre $p - 1$. Dans un système réduit des résidus modulo p il existe exactement $\varphi(d)$ nombres d'ordre d.*

Démonstration. Soit B le système réduit des résidus modulo p. Soit d un certain diviseur naturel du nombre $p - 1$. Notons $\psi(d)$ le nombre d'éléments de B dont l'ordre vaut d. Supposons qu'il existe au moins un élément $a \in B$ dont l'ordre est p, c'est-à-dire $\psi(d) > 0$. Alors, $a, a^2, \ldots, a^d$ sont des solutions modulo p distinctes de la congruence

(1) $\quad x^d \equiv 1 \pmod p$

et, selon le théorème 4.6, il n'y a pas d'autres solutions. Par suite, tous les résidus d'ordre d doivent appartenir à l'ensemble

$$M = \{a, a^2, \ldots, a^d\}.$$

Selon les propositions 5.7 et 5.8, le nombre a^k est d'ordre d si et seulement si $(d, k) = 1$. Il s'ensuit que $\psi(d) = \varphi(d)$ au cas où il existe au moins un élément d'ordre d. Ainsi

(2) $\quad \psi(d) \leqslant \varphi(d)$ pour tout diviseur d du nombre $(p - 1)$.

Chaque résidu possédant un ordre d, diviseur de $p - 1$, on a

$$\sum_{d \mid (p-1)} \psi(d) = p - 1.$$

D'autre part, selon le théorème 3.11,

$$\sum_{d \mid (p-1)} \varphi(d) = p - 1,$$

donc

(3) $$\sum_{d \mid (p-1)} (\varphi(d) - \psi(d)) = 0.$$

Sur la base de (2) et (3) on conclut que $\psi(d) = \varphi(d)$ pour tout diviseur naturel d du nombre $p - 1$. □

Si le résidu a modulo m est d'ordre $\varphi(m)$, on appelle alors a *racine primitive modulo m*.

THÉORÈME 5.10. *Un groupe des résidus modulo p premiers avec le module est cyclique. Le nombre de racines primitives modulo p vaut* $\varphi(p-1)$.

Ce théorème découle directement du théorème précédent selon lequel il existe $\varphi(p-1)$ générateurs du groupe des résidus premiers avec p.

Si g est la racine primitive modulo p, les $p-1$ puissances

(1) $g, g^2, \ldots, g^{p-1}$

sont alors non congrues modulo p. Par conséquent, la proposition suivante est vraie.

PROPOSITION 5.11. *Si g est une racine primitive modulo p, les p — 1 puissances* $g, g^2, \ldots, g^{p-1}$ *constituent alors un système réduit des résidus modulo p.*

Les racines primitives n'existent pas pour tout module m, mais seulement pour $m = 2, 4, p^k, 2p^k$ (p étant un nombre premier impair).

Exemple. Soit $p = 13$. Cherchons les racines primitives suivant ce module.

Le nombre $p - 1 = 12$ possède 6 diviseurs naturels: 1, 2, 3, 4, 6, 12:

$$\varphi(1) = 1, \quad \varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2, \quad \varphi(6) = 2, \quad \varphi(12) = 4.$$

Les nombres 2, 6, 7, 11 sont des racines primitives modulo 13. Le nombre 12 a l'ordre 2; le nombre 3 l'ordre 3; les nombres 5, 8 l'ordre 4; les nombres 4, 10 l'ordre 6, le nombre 1 l'ordre 1.

Indices suivant un module simple. Soit g une racine primitive modulo p. Alors, les nombres

(1) $g, g^2, \ldots, g^{p-1}$

forment un système réduit des résidus modulo p. Aussi tout nombre a est-il premier avec p et n'est congru qu'avec un et seulement un des nombres de la série (1).

Si $a \equiv g^k \pmod p$, alors k est dit *indice du nombre a modulo p* affectant la base g et est désigné par le symbole ind a ou $\text{ind}_g\, a$. Si k' est un autre nombre pour lequel $a \equiv g^{k'} \pmod p$, alors $g^k \equiv g^{k'} \pmod p$ et, selon la proposition 5.4, $k \equiv k' \pmod{(p-1)}$. Ainsi, l'ensemble des indices d'un nombre a donné forment une classe résiduelle modulo $p - 1$. Par définition de l'indice, $a \equiv b \pmod p$ implique ind $a \equiv$ ind $b \pmod{p-1}$.

Exemple. Soit $p = 13$. Le nombre 2 est la racine primitive modulo 13. Les indices des nombres 1, 2, . . ., 12 affectant la base $g = 2$ sont:

a	1	2	3	4	5	6	7	8	9	10	11	12
ind a	0	1	4	2	9	5	11	3	8	10	7	6

A l'aide de ce tableau, la base du nombre a étant donnée, on obtient son indice modulo 13. Le tableau qui suit permet, connaissant l'indice, d'obtenir le nombre correspondant:

ind a	0	1	2	3	4	5	6	7	8	9	10	11
a	1	2	4	8	3	6	12	11	9	5	10	7

Au moyen d'indices on est en mesure de réduire une multiplication modulo p à une addition modulo $p - 1$ de façon analogue au procédé qui permet à l'aide des logarithmes de réduire une multiplication banale des nombres à une addition.

THÉORÈME 5.12. *Si les nombres a, b sont premiers avec p et n est un nombre naturel quelconque, alors*

$$\text{(1)}\quad \begin{aligned} &\operatorname{ind} ab \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{p-1},\\ &\operatorname{ind} a^n \equiv n \operatorname{ind} a \pmod{p-1}. \end{aligned}$$

Démonstration. Par définition des indices des nombres a et b, on a:

$$a \equiv g^{\operatorname{ind} a} \pmod{p}, \qquad b \equiv g^{\operatorname{ind} b} \pmod{p},$$

de là on tire le produit

$$ab \equiv g^{\operatorname{ind} a + \operatorname{ind} b} \pmod{p}.$$

Donc, ind a + ind b est l'un des indices du produit ab, c'est-à-dire

$$\operatorname{ind} ab \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{p-1}.$$

De la congruence $a \equiv g^{\operatorname{ind} a} \pmod{p}$ il s'ensuit que

$$a^n \equiv g^{n \operatorname{ind} a} \pmod{p};$$

aussi n ind a est-il l'un des indices de la puissance a^n, c'est-à-dire

$$\operatorname{ind} a^n \equiv n \operatorname{ind} a \pmod{p-1}. \ \square$$

Exemples. 1. Soient $p = 13$, $a = 8$, $b = 6$; alors ind $8 = 9$, ind $6 = 8$, ind $8 \cdot 6 \equiv 9 + 8 \equiv 5 \pmod{12}$.

2. Résoudre la congruence $6x \equiv 7 \pmod{13}$.

La congruence donnée est équipotente à:

$$\operatorname{ind} 6 + \operatorname{ind} x = \operatorname{ind} 7 \pmod{12} \text{ ou } \operatorname{ind} x \equiv \equiv \operatorname{ind} 7 - \operatorname{ind} 6 = 11 - 5 = 6 \pmod{12}.$$

Il s'ensuit que $x \equiv 12 \pmod{13}$.

THÉORÈME 5.12. *Soient $\mathcal{G}_p$ un groupe multiplicatif des classes résiduelles, éléments premiers avec p et C un groupe additif des classes résiduelles modulo $p - 1$. L'application a mod $p \mapsto$ ind a (mod $p - 1$), associant à chaque élément a du groupe $\mathcal{G}_p$ l'élément ind a du groupe C, est un isomorphisme du groupe $\mathcal{G}_p$ sur le groupe C.*

D é m o n s t r a t i o n. Par définition de l'indice, la correspondance $a \bmod p \overset{\varphi}{\mapsto} \operatorname{ind} a \pmod{p-1}$ est bijective. En outre, dans le groupe $\mathcal{G}_p$ est respectée l'opération de multiplication, car de la congruence

$$\operatorname{ind} ab = \operatorname{ind} a + \operatorname{ind} b \pmod{p-1}$$

il s'ensuit que

$$[\operatorname{ind} ab] = [\operatorname{ind} a] + [\operatorname{ind} p].$$

Par conséquent, φ est un isomorphisme du groupe $\mathcal{G}_p$ sur le groupe C. □

En arithmétique courante le fondement de la théorie des logarithmes est un isomorphisme du groupe multiplicatif des nombres réels positifs et du groupe additif de tous les nombres réels. Le théorème démontré, constituant le fondement de la théorie des indices, permet de comprendre pourquoi la théorie des logarithmes (de l'arithmétique courante) ressemble à la théorie des indices (suivant un module simple).

Congruences binomiales. On appelle *congruence binomiale* la congruence de la forme

(1) $ax^n \equiv b \pmod{p}$,

où l'exposant n est positif. Si p est premier, la congruence (1) est équipotente à la congruence

(2) $n\xi \equiv \operatorname{ind} b - \operatorname{ind} a \pmod{p-1}$, où $\xi = \operatorname{ind} x$.

Pour que la congruence (2) soit résoluble il faut et il suffit que le nombre $d = (n, p-1)$ divise la différence $\operatorname{ind} b - \operatorname{ind} a$. Si cette condition est remplie, la congruence (2) admet d solutions modulo $p-1$; par conséquent, la congruence (1) possède exactement d solutions modulo p.

E x e m p l e. Résolvons la congruence

(3) $6x^8 \equiv 5 \pmod{13}$.

La congruence (2) prend dans ce cas la forme

$$8\xi \equiv \operatorname{ind} 5 - \operatorname{ind} 6 \pmod{12} \text{ ou } 8\xi \equiv 4 \pmod{12}.$$

Cette dernière congruence est compatible, vu que (8, 12) divise 4 et admet les quatre solutions suivantes:

$$\xi \equiv 2, 5, 8, 11 \pmod{12}; \qquad \operatorname{ind} x \equiv 2, 5, 8, 11 \pmod{12}.$$

Donc, la congruence (3) possède quatre solutions:

$$x \equiv 4, 6, 9, 7 \pmod{13}.$$

La congruence binomiale (1) peut être réduite à une plus simple en multipliant les deux membres de la congruence par le nombre a',

inverse de a modulo p, $a'a \equiv 1 \pmod p$. La multiplication effectuée, on obtient $x^n \equiv a'b \pmod p$. Ainsi, toute congruence binomiale peut être réduite à la forme la plus simple:

$$x^m \equiv c \pmod p.$$

DÉFINITION. Le nombre a est appelé *k-naire résidu modulo m* si la congruence $x^k \equiv a \pmod m$ admet au moins une solution.

Soient p un nombre premier et $\bar{k} = (k, p-1)$.

THÉORÈME 5.13. *Pour tout résidu a suivant un module simple p les affirmations suivantes sont équipotentes:*

(α) *a est un k-naire résidu modulo p;*

(β) $a^{\frac{p-1}{\bar{k}}} \equiv 1 \pmod p$;

(γ) *l'ordre de la classe résiduelle a* mod p *est un diviseur du nombre $\frac{p-1}{\bar{k}}$, c'est-à-dire* $\mathcal{O}(a \bmod p) \mid ((p-1)/\bar{k})$;

(δ) ind a *est un multiple de $\bar{k}$.*

D é m o n s t r a t i o n. (α) $\to$ (β). Soit a le k-naire résidu; alors, il existe un résidu x_0 premier avec p vérifiant la congruence $x_0^k \equiv a \pmod p$. Donc,

$$a^{\frac{p-1}{\bar{k}}} \equiv (x_0^k)^{\frac{p-1}{\bar{k}}} \equiv (x_0^{k/\bar{k}})^{p-1} \equiv 1 \pmod p,$$

c'est-à-dire que (β) est vérifiée;

(β) $\to$ (γ). Selon la proposition 5.2, de la congruence (β) s'ensuit (γ);

(γ) $\to$ (δ). De la condition (γ) il s'ensuit que

$$(1) \quad a^{\frac{p-1}{\bar{k}}} \equiv 1 \pmod p.$$

Soit g une racine primitive modulo p. Alors, $a = g^{\operatorname{ind} a}$ et, en vertu de (1),

$$(g^{\operatorname{ind} a})^{\frac{p-1}{\bar{k}}} \equiv g^{\operatorname{ind} a \cdot \frac{p-1}{\bar{k}}} \equiv 1 \pmod p.$$

Donc, selon la proposition 5.2,

$$\operatorname{ind} a \cdot \frac{p-1}{\bar{k}} \equiv 0 \pmod{p-1};$$

et, par suite, $\bar{k} \mid \operatorname{ind} a$, c'est-à-dire qu'est remplie (δ).

(δ) $\to$ (α). Considérons la congruence

$$k\xi \equiv \operatorname{ind} a \pmod{p-1}.$$

Etant donné que $\bar{k} = (k, p - 1) \mid \text{ind}\, a$, la congruence admet une solution. Soit ξ_0 la solution de cette congruence, $k\xi_0 \equiv \text{ind}\, a \times$ $\times \pmod{p-1}$. Alors, $g^{k\xi_0} \equiv g^{\text{ind}\, a} \pmod{p}$, par conséquent, $(g^{\xi_0})^k \equiv a \pmod{p}$, c'est-à-dire a est le k-naire résidu modulo p. Ainsi, $(\delta) \to (\alpha)$. □

Exercices

1. Composer le tableau des indices modulo 19 de base 2.
2. Composer le tableau des indices modulo 29 de base 10.
3. Chercher les racines primitives des nombres 41 et 49.
4. Soient p un nombre premier impair et $n > 1$. Montrer qu'il existe exactement $(p-1)\cdot\varphi(p-1)$ racines primitives différentes du nombre p^n non congrues modulo p^2.
5. Si p est un nombre premier impair, $n > 1$, il existe exactement $\varphi(\varphi(p^n))$ racines primitives différentes du nombre p^n.
6. Montrer que si p est un nombre premier impair et $n > 1$ il existe exactement $\varphi(\varphi(p^n))$ racines primitives différentes du nombre $2p^n$.
7. Chercher l'indice du nombre (-1) suivant un module simple impair p, la base étant quelconque.
8. Montrer que pour un nombre premier de la forme $2^n + 1$ avec $n > 3$, le nombre 3 est une racine primitive.
9. Montrer que si p est un nombre premier de la forme $4k + 1$ et g la racine primitive modulo p, $p - g$ est aussi une racine primitive modulo p.

§ 6. Conversion d'une fraction ordinaire en fraction systématique et appréciation de la longueur de la période d'une fraction systématique

Une fraction périodique m-naire

$$m^h\left(b_1 m^{l-1} + \ldots + b_l + \frac{a_1}{m} + \ldots + \frac{a_k}{m^k} + \right.$$
$$\left. + \frac{a_1}{m^{k+1}} + \ldots + \frac{a_k}{m^{2k}} + \ldots\right)$$

s'écrit de façon condensée sous forme

$$(*) \qquad m^h\,(b_1 \ldots b_l, \overline{a_1 \ldots a_k}).$$

$a_1 \ldots a_k$ est dans ce cas appelé *période de la fraction* et $b_1 \ldots b_l$ *prépériode de la fraction*. Le nombre k est la *longueur de la période* et le nombre l la *longueur de la prépériode*.

La fraction périodique m-naire (*) est dite *normée* si sont remplies les conditions:

(α) $a_k \neq b_l$;

(β) la période $a_1 \ldots a_k$ possède la plus petite longueur possible.

Si a est la fraction périodique normée m-naire (*), c'est-à-dire si $a = m^h\,(b_1 \ldots b_l, \overline{a_1 \ldots a_k})$, on dit alors que la fraction

$m^h\ (b_1 \ldots b_l,\ a_1 \ldots a_k)$ est *la décomposition normée du nombre a en une fraction périodique m-naire.*

PROPOSITION 6.1. *Soit m un nombre naturel fixé supérieur à l'unité. Pour tout nombre rationnel positif donné a il existe un entier h et des nombres naturels c, n tels que*

$$\text{(I)} \quad a = m^h \frac{c}{n}, \quad (m, n) = 1, \quad m \nmid c, \quad (c, n) = 1.$$

En outre, si l'entier h_1 et les nombres naturels c_1, n_1 satisfont aux conditions

$$\text{(I}'\text{)} \quad a = m^{h_1} \frac{c_1}{n_1}, \quad (m, n_1) = 1, \quad m \nmid c_1, \quad (c_1, n_1) = 1,$$

alors, $h = h_1$, $c = c_1$ *et* $n = n_1$.

Démonstration. Figurons le nombre rationnel a sous forme d'une fraction irréductible $a = u/v$, $(u, v) = 1$, $u, v \in \mathbf{N}$. Notons n le plus grand diviseur naturel du dénominateur v, premier avec m, $v = qn$. Alors, chaque diviseur premier du nombre q divisera m; il existe donc des entiers t tels que $\frac{m^t}{q} \in \mathbf{N}$. Notons t_0 le plus petit entier tel que $\frac{m^{t_0}}{q} u \in \mathbf{N}$. Soit $c = \frac{m^{t_0}}{q} \cdot u$, alors

$$a = m^{-t_0} \cdot \frac{c}{n}, \quad m \nmid c, \quad (c, n) = 1.$$

En posant $h = -t_0$, on voit que les nombres h, c, n satisfont aux conditions (I).

Supposons que les nombres h_1, c_1, n_1 remplissent les conditions (I'); alors $a = m^h \cdot \frac{c}{n} = m^{h_1} \cdot \frac{c_1}{n_1}$. Posons $h \geqslant h_1$, alors $m^{h-h_1} cn_1 = c_1 n$. Vu que, par hypothèse, $(m, n) = 1$ et $m \nmid c_1$, on a $m \nmid c_1 n$; donc $h - h_1 = 0$ et $cn_1 = c_1 n$ et, par suite, $h = h_1$ et $\frac{c}{n} = \frac{c_1}{n_1}$. $\frac{c}{n} = \frac{c_1}{n_1}$ étant irréductibles, $c = c_1$ et $n = n_1$. □

COROLLAIRE 6.2. *Pour un m fixé et un nombre a rationnel et positif donné, il existe un unique entier h, tel que la fraction a/m^h ait un dénominateur premier avec m et un numérateur non divisible par m.*

DÉFINITION. La figuration du nombre rationnel positif a sous forme de

$$\text{(I)} \quad a = m^h \cdot \frac{c}{n},$$

où $(m, n) = 1$, $m \nmid c$, $(c, n) = 1$, $(c, n) \in N$ sera dite *m-figuration du nombre a.* Le nombre h sera également noté $h(a)$.

PROPOSITION 6.3. *Si une fraction périodique m-naire*

$$m^h\,(b_1 \ldots b_l,\ \overline{a_1 \ldots a_k})$$

satisfait à la condition $a_k \neq b_l$, *alors sa prépériode a la plus petite longueur possible.*

Démonstration. En effet, si $a_k = b_l$ et $l > 1$, alors

$$m^h (b_1 \ldots b_l, \overline{a_1 \ldots a_k}) = m^{h+1} (b_1 \ldots b_{l-1}, \overline{a_k a_1 \ldots a_{k-1}}),$$

c'est-à-dire qu'on peut diminuer la longueur de la prépériode de la fraction. □

Proposition 6.4. *Supposons que la fraction*

(I) $m^h (b_1 \ldots b_l, \overline{a_1 \ldots a_k})$

soit la décomposition en fraction périodique m-naire du nombre rationnel positif a. Soit

(II) $a = m^{h(a)} \cdot \frac{c}{n}$

une m-figuration du nombre a. Dans ce cas les affirmations suivantes sont équipotentes

(α) $b_l \neq a_k$;

(β) $A \not\equiv B \pmod{n}$,

où $B = b_1 m^{l-1} + \ldots + b_l$ *et* $A = a_1 m^{k-1} + \ldots + a_k$;

(γ) $h = h(a)$;

(δ) $\frac{a}{m^h} = \frac{c}{n} = b_1 \ldots b_l, \overline{a_1 \ldots a_k}$.

Démonstration. (α) → (β). Définissons les nombres A et B au moyen des égalités suivantes:

(1) $A = a_1 m^{k-1} + \ldots + a_k, \quad 0 \leqslant a_1, \ldots, a_k < m,$

(2) $B = b_1 m^{l-1} + \ldots + b_l, \quad 0 \leqslant b_1, \ldots, b_l < m.$

Vu que $0 \leqslant b_l, a_k < m$, on déduit de (α) que

(3) $a_k \not\equiv b_l \pmod{m}$.

Sur la base de (1), (2) et (3) on conclut que

$$A \not\equiv B \pmod{m};$$

c'est-à-dire qu'il y a lieu (β).

(β) → (γ). Selon l'hypothèse,

$$a = m^h (b_1 \ldots b_l, \overline{a_1 \ldots a_k}) = \\ = m^h \left(b_1 m^{l-1} + \ldots + b_l + \frac{a_1 m^{k-1} + \ldots + a_k}{m^k - 1} \right),$$

par suite,

(4) $a = m^h \left(B + \frac{A}{m^k - 1} \right) = m^h \frac{B(m^k - 1) + A}{m^k - 1}$.

On constate sans peine que

$$B(m^k - 1) + A \equiv -B + A \equiv -b_l + a_k \pmod{m}.$$

Selon la condition (β) il s'ensuit que

(5) $B(m^k - 1) + A \not\equiv 0 \pmod{m}$,

c'est-à-dire que $m \nmid (B(m^k - 1) + A)$. En outre, en raison de (II) et de (4), on a

(6) $a = m^{h(a)} \cdot \frac{c}{n} = m^h \cdot \frac{B(m^k-1)+A}{m^k-1}$.

En vertu de la proposition 6.1, de (5) et de (6) s'ensuit l'égalité

(7) $h = h(a)$;

(γ) → (δ). Par hypothèse,

(8) $a = m^{h(a)} \cdot \frac{c}{n} = m^h (b_1 \ldots b_l, \overline{a_1 \ldots a_k})$.

De (7) et (8) il vient

(9) $\frac{a}{m^h} = \frac{c}{n} = b_1 \ldots b_l, \overline{a_1 \ldots a_k}$,

et, par suite, est satisfait (δ).

(δ) → (α). De la condition (δ) s'ensuit que

$$\frac{c}{n} = \frac{B(m^k-1)+A}{m^k-1},$$

c'est-à-dire $B(m^k-1)+A = c \cdot \frac{m^k-1}{n}$. Vu que $(c, m) = 1$ et $\left(\frac{m^k-1}{n}, m\right) = 1$, $B(m^k-1)+A \equiv -B+A \not\equiv 0 \pmod{m}$. En outre, $-B+A \equiv -b_l + a_k \pmod{m}$. Donc, $b_l \not\equiv a_k \pmod{m}$. En vertu de (1), (2), il s'ensuit que $b_l \neq a_k$. □

Proposition 6.5. *Soit* $0, \overline{a_1, \ldots, a_k}$ *la décomposition en fraction périodique m-naire du nombre rationnel positif* r/n, $(r, n) = 1$, c'est-à-dire

(1) $r/n = 0, \overline{a_1 \ldots a_k}$.

Alors, la longueur k de la période est divisible par l'ordre de la classe résiduelle $m \bmod n$, $\Theta(m \bmod n) \mid k$.

Démonstration. Par hypothèse,

(2) $\frac{r}{n} = \frac{a_1}{m} + \ldots + \frac{a_k}{m^k} + \frac{a_1}{m^{k+1}} + \ldots + \frac{a_k}{m^{2k}} + \ldots$

Posons

$$A = a_1 m^{k-1} + \ldots + a_k.$$

Alors, (2) peut être écrit sous forme

$$\frac{r}{n}=\frac{A}{m^k}+\frac{A}{m^{2k}}+\dots$$

Donc,

(3) $$\frac{r}{n}=\frac{A}{m^k-1}$$

et $r(m^k-1)=nA$. Or, comme $(n, r)=1$, on a $n \mid (m^k-1)$, c'est-à-dire

(4) $$m^k\equiv 1 \pmod n.$$

En vertu de la proposition 5.2, il s'ensuit de (4) que k est divisible par l'ordre de la classe résiduelle m mod n. □

THEOREME 6.6. *Un nombre rationnel* $\frac{r}{n}>0$, $(r, n)=1$, *se décompose en fraction purement périodique m-naire avec la plus petite période*

(1) $$0,\overline{a_1\dots a_k},$$

si et seulement si sont remplies les conditions

(2) $$0<\frac{r}{n}\leqslant 1,\qquad (m, n)=1.$$

Dans ce cas la longueur k de la plus petite période est égale à l'ordre de la classe résiduelle m mod n *et la suite* $a_1, \dots, a_k$ *coïncide avec la suite des chiffres en figuration m-adique du nombre* $(m^k-1)\cdot r/n$.

D é m o n s t r a t i o n. Soit donné un nombre rationnel positif a représenté par une fraction irréductible r/n satisfaisant aux conditions (2). Posons $k=\Theta$ (m mod n). En multipliant le numérateur et le dénominateur de la fraction $\frac{r}{n}$ par $\frac{m^k-1}{n}$, il vient

(3) $$a=\frac{r}{n}=\frac{A}{m^k-1}.$$

Soit

(4) $$A=a_1m^{k-1}+\dots+a_k$$

une figuration m-adique du nombre a. En raison de (3)

(5) $$a=\frac{r}{n}=\frac{A}{m^k}+\frac{A}{m^{2k}}+\dots$$

De (4) et (5) il s'ensuit que

$$a=\frac{a_1}{m}+\dots+\frac{a_k}{m^k}+\frac{a_1}{m^{k+1}}+\dots+\frac{a_k}{m^{2k}}+\dots,$$

autrement dit, on a obtenu une décomposition du nombre a en une fraction purement périodique dont la période est de longueur k:

$$a = 0,\ \overline{a_1 \ldots a_k}.$$

De plus, en vertu de la proposition 6.5, la longueur k de la période est minimale et la suite $a_1, \ldots, a_k$ coïncide avec la suite des chiffres dans la figuration m-adique du nombre $(m^k - 1)\cdot r/n$.

Supposons à présent qu'on est en possession de la décomposition du nombre $\frac{r}{n}$, $(r, n) = 1$, en une fraction purement périodique à période minimale, $\frac{r}{n} = 0,\ \overline{a_1 \ldots a_k}$, c'est-à-dire

(1) $$\frac{r}{n} = \frac{a_1}{m} + \ldots + \frac{a_k}{m^k} + \frac{a_1}{m^{k+1}} + \ldots + \frac{a_k}{m^{2k}} + \ldots$$

Soit

(6) $$A = a_1 m^{k-1} + \ldots + a_k.$$

Alors,

(7) $$\frac{r}{n} = \frac{A}{m^k} + \frac{A}{m^{2k}} + \ldots$$

et, partant,

(8) $$\frac{r}{n} = \frac{A}{m^k - 1}.$$

En raison de (7) et (8), on a $0 < A \leqslant m^k - 1$. De là, ainsi que de (8), il s'ensuit que

$$0 < \frac{r}{n} \leqslant 1.$$

De (8) on déduit que $r(m^k - 1) = An$ et, comme $(n, r) = 1$, on a $n \mid (m^k - 1)$, c'est-à-dire

(9) $$m^k \equiv 1 \pmod{n}$$

et, partant, $(m, n) = 1$. De (9), selon la proposition 5.2, il s'ensuit que $\Theta\ (m \bmod n) \mid k$. Par hypothèse, k est la plus petite période, donc, en vertu de la proposition 6.5, $k = \Theta\ (m \bmod n)$. En raison de (8), $A = (m^k - 1)\cdot\frac{r}{n}$. Ensuite, en raison de (2),

$$(m^k - 1)\cdot\frac{r}{n} = a_1 m^{k-1} + \ldots + a_k.$$

Ainsi, la suite $a_1, \ldots, a_k$ des chiffres de la période de la fraction $0,\ \overline{a_1 \ldots a_k}$ coïncide avec la suite des chiffres de la figuration m-adique du nombre $(m^k - 1)\cdot\frac{r}{n}$. □

THÉORÈME 6.7. *Tout nombre rationnel positif a est doué d'une décomposition normée en fraction périodique m-naire* $m^h(b_1 \ldots \ldots b_l, \overline{a_1 \ldots a_k})$. *De plus, si* $a = m^{h(a)} \cdot \frac{c}{n}$ *est une m-figuration du nombre a, alors:*

1) $h = h(a)$;

2) $k = \Theta(m \mod n)$;

3) *la suite* $b_1, \ldots, b_l$ *coïncide avec la suite des chiffres dans la figuration m-adique du nombre B, où*

$$B = \begin{cases} \left[\frac{a}{m^h}\right] & si \ \frac{a}{m^h} \notin \mathbf{Z}, \\ \frac{a}{m^h} - 1 & si \ \frac{a}{m^h} \in \mathbf{Z}; \end{cases}$$

4) *la suite* $a_1, \ldots, a_k$ *coïncide avec la suite des chiffres dans la figuration m-adique du nombre A, où*

$$A = (m^k - 1)\left(\frac{a}{m^h} - B\right).$$

D é m o n s t r a t i o n. Selon la proposition 6.1, il existe pour le nombre a un entier h et des nombres naturels c, n tels que

(1) $a = m^h \cdot \frac{c}{n}$, $(m, n) = 1$, $m \nmid c$, $(c, n) = 1$.

Le nombre c peut être figuré sous forme de $c = Bn + r$, où $0 < r \leqslant n$, $(r, n) = 1$, B étant un nombre naturel, donc,

(2) $\frac{c}{n} = B + \frac{r}{n}$, $0 < \frac{r}{n} \leqslant 1$.

Par conséquent, il vient:

$$B = \begin{cases} \left[\frac{a}{m^h}\right] & \text{si } \frac{a}{m^h} \notin \mathbf{Z}, \\ \frac{a}{m^h} - 1 & \text{si } \frac{a}{m^h} \in \mathbf{Z}. \end{cases}$$

Selon le théorème 6.6, la fraction propre r/n se décompose en une fraction m-naire purement périodique

(3) $\frac{r}{n} = 0, \overline{a_1 \ldots a_k}$.

De plus, la longueur k de la plus petite période est égale à l'ordre de la classe résiduelle m mod n,

(4) $k = \Theta(m \mod n)$,

et la suite $a_1, \ldots, a_k$ coïncide avec la suite des chiffres dans la figuration m-adique du nombre A, où

$$A=(m^k-1)\cdot\frac{r}{n}=(m^k-1)\left(\frac{a}{m^h}-B\right).$$

Soit $B = b_1m^{l-1} + \ldots + b_l$ une figuration m-adique du nombre B. Alors, en vertu de (1), (2) et (3), il vient

$$(5)\qquad \frac{a}{m^h}=\frac{c}{n}=b_1\ \ldots\ b_l,\ \overline{a_1\ \ldots\ a_k},$$

par suite,

$$(6)\qquad a=m^h(b_1\ \ldots\ b_l,\ \overline{a_1\ \ldots\ a_k}).$$

Vu que $h = h\,(a)$, il s'ensuit de (6), selon la proposition 6.4, l'inégalité $b_l \neq a_k$. En outre, en raison de (4) et de la proposition 6.5, la longueur k de la période dans la décomposition (6) est minimale. Ainsi, (6) est une décomposition normée du nombre a en une fraction périodique m-naire. □

Exercices

1. Chercher combien y a-t-il de chiffres dans la période des fractions décimales en lesquelles sont converties les fractions ordinaires dont les dénominateurs sont: 3, 7, 11, 13, 17, 19, 21.

2. Convertir les fractions périodiques décimales suivantes en fractions ordinaires: 0,35 (62); 5,1 (538); 3, (27); 11,12 (31).

3. Chercher le dénominateur de la fraction se convertissant en une fraction purement périodique et possédant trois chiffres dans la période.

4. Soit p un nombre premier autre que 2 et 5. Montrer que si la fraction $1/p$ est convertible en une fraction décimale purement périodique avec un nombre pair de chiffres dans la période, alors les chiffres de la seconde moitié de la période complètent jusqu'à neuf les chiffres correspondants de la première moitié de la période. Par exemple, $1/7 = 0,\overline{142857}$.

5. Chercher combien y a-t-il de chiffres dans la période des fractions décimales en lesquelles sont converties les fractions ordinaires dont les dénominateurs sont: 41, 13·37, 11·13·17, 5·7·19, 2·11·13.

6. Quelle valeur est susceptible de prendre le dénominateur d'une fraction se convertissant en une fraction décimale purement périodique avec trois chiffres dans la période?

7. Quelle est la valeur du dénominateur d'une fraction qu'on peut convertir en fraction décimale purement périodique avec cinq chiffres dans la période?

CHAPITRE XIII

ANNEAUX

§ 1. Idéaux d'un anneau. Anneau quotient

Idéaux d'un anneau. Soient $\mathcal{K} = \langle K, +, -, \cdot, 1 \rangle$ un anneau et I un sous-ensemble de l'ensemble K. L'ensemble I est dit *fermé dans* $\mathcal{K}$ *par rapport à la soustraction* si $a - b \in I$ pour tous éléments a et b de I.

L'ensemble I est dit *stable par rapport à la multiplication à droite par les éléments de l'anneau* $\mathcal{K}$ si $ak \in I$ pour tout a de I et tout k de K, c'est-à-dire si dans l'ensemble I, avec chaque élément a de ce dernier, sont inclus tous ses multiples à droite ak, où $k \in K$. On définit de façon analogue l'ensemble stable par rapport à la multiplication à gauche par les éléments de l'anneau $\mathcal{K}$.

L'ensemble I est dit *stable par rapport à la multiplication par les éléments de l'anneau* $\mathcal{K}$ s'il est stable par rapport à la multiplication à droite et à gauche par les éléments de l'anneau $\mathcal{K}$.

DEFINITION. On appelle *idéal à droite* (*à gauche*) *de l'anneau* $\mathcal{K}$ tout sous-ensemble non vide de l'ensemble K fermé dans $\mathcal{K}$ par rapport à la soustraction et stable par rapport à la multiplication à droite (à gauche) par les éléments de l'anneau $\mathcal{K}$.

DEFINITION. On appelle *idéal bilatéral de l'anneau* $\mathcal{K}$ ou tout simplement *idéal de l'anneau* $\mathcal{K}$ tout sous-ensemble non vide de l'ensemble K si ce sous-ensemble est en même temps un idéal à droite et à gauche de l'anneau $\mathcal{K}$.

Il s'ensuit de la définition que tout idéal I de l'anneau $\mathcal{K}$ renferme le zéro de l'anneau et est fermé relativement aux trois premières opérations principales de l'anneau. L'algèbre $\langle I, +, - \rangle$ est un *sous-groupe* du groupe additif $\langle K, +, - \rangle$ de l'anneau. L'ensemble $\{0_{\mathcal{K}}\}$ est un idéal de l'anneau $\mathcal{K}$ appelé *idéal nul* ou *zéro*. L'ensemble K est également un idéal de l'anneau $\mathcal{K}$; il est composé des multiples de l'unité de l'anneau et, par suite, est appelé *idéal unité* (ou *unitaire*) *de l'anneau* $\mathcal{K}$. Les idéaux zéro et unité sont dits *idéaux triviaux de l'anneau* $\mathcal{K}$. Les idéaux de l'anneau distincts des idéaux triviaux sont dits *idéaux propres de l'anneau.*

E x e m p l e s. 1. Soient $\mathfrak{Z}$ un anneau des entiers et n un entier fixé. L'ensemble $nZ = \{nx \mid x \in Z\}$ est un idéal de l'anneau $\mathfrak{Z}$.

2. Soient $\mathcal{K}$ un anneau quelconque et n un entier fixé. L'ensemble $nK = \{nx \mid x \in K\}$ est un idéal de l'anneau $\mathcal{K}$.

3. Soient $\mathcal{K}$ un anneau commutatif et a son élément fixé. L'ensemble $\{ka \mid k \in K\}$ composé des multiples de l'élément a est un idéal. Il est appelé *idéal principal engendré par l'élément* a et noté (a). Dans les anneaux non commutatifs il est nécessaire de distinguer les idéaux principaux à droite des idéaux principaux à gauche.

4. Soient $\mathcal{K}$ un anneau commutatif et $a_1, \ldots, a_n \in K$. L'ensemble $\{k_1a_1 + \ldots + k_na_n \mid k_1, \ldots, k_n \in K\}$ est un idéal de l'anneau $\mathcal{K}$. On l'appelle *idéal engendré par les éléments* $a_1, \ldots$ $\ldots, a_n$ et est désigné par le symbole $(a_1, \ldots, a_n)$.

Dans les anneaux non commutatifs il est nécessaire de distinguer les idéaux à droite des idéaux à gauche engendrés par les éléments $a_1, \ldots, a_n$.

Etudions les opérations sur les idéaux. On appelle *intersection des idéaux* I et J de l'anneau $\mathcal{K}$ l'ensemble $I \cap J$. On définit de façon analogue l'intersection de toute collection d'idéaux de l'anneau. On vérifie sans peine que l'intersection de toute collection d'idéaux de l'anneau est un idéal de cet anneau.

On appelle *somme des idéaux* I et J l'ensemble $I + J$ défini par l'égalité

$$I + J = \{x + y \mid x \in I, y \in J\}.$$

On vérifie aisément que la somme des idéaux de l'anneau est un idéal de cet anneau. L'addition des idéaux est douée des propriétés de commutativité et d'associativité.

On appelle *produit des idéaux* I et J de l'anneau $\mathcal{K}$ l'ensemble de tous les éléments de la forme $x_1y_1 + \ldots + x_ny_n$, où $x_i \in I$, $y_i \in J$ et n un entier positif quelconque. Le produit des idéaux I et J est noté $I \cdot J$. On vérifie sans peine que le produit des idéaux de l'anneau est un idéal de cet anneau.

Notons que l'idéal principal (a) engendré par l'élément a d'un anneau commutatif $\mathcal{K}$ est une *intersection de tous les idéaux renfermant l'élément* a et, par suite, (a) est le plus petit des idéaux contenant a.

De façon analogue, l'idéal $(a_1, \ldots, a_n)$ engendré par les éléments $a_1, \ldots, a_n$ de l'anneau commutatif $\mathcal{K}$ est une *intersection de tous les idéaux renfermant les éléments* $a_1, \ldots, a_n$, et, par suite, $(a_1, \ldots, a_n)$ est le plus petit des idéaux contenant $a_1, \ldots, a_n$.

Congruences et classes résiduelles suivant l'idéal. Soit I un idéal fixé de l'anneau $\mathcal{K}$.

DEFINITION. Les éléments a, b de l'anneau $\mathcal{K}$ sont dits *congrus suivant l'idéal* I si $a - b \in I$.

La notation $a \equiv b \pmod{I}$ signifie que les éléments a et b sont congrus suivant l'idéal I.

PROPOSITION 1.1. *La congruence suivant l'idéal* I *dans l'anneau* $\mathcal{K}$ *(sur l'ensemble* K*) est une relation d'équivalence.*

D é m o n s t r a t i o n. La congruence suivant l'idéal I est réflexive, vu que $a - a \in I$ pour tout élément a de K. La congruence suivant l'idéal I est transitive, vu que de $a - b \in I$ et $b - c \in I$ il s'ensuit que

$$a - c = (a - b) + (b - c) \in I.$$

La congruence suivant l'idéal I est symétrique, vu que de $a - b \in I$ s'ensuit $b - a \in I$. □

DÉFINITION. Les classes d'équivalence de la congruence suivant l'idéal I dans l'anneau $\mathcal{K}$ sont dénommées *classes résiduelles suivant l'idéal I* ou *classes de l'anneau $\mathcal{K}$ suivant l'idéal I*.

La classe résiduelle contenant l'élément a de l'anneau $\mathcal{K}$ sera notée $\bar{a}$. Apparemment, $\bar{a} = a + I$.

THÉORÈME 1.2. *Les classes résiduelles de l'anneau $\mathcal{K}$ suivant l'idéal I sont douées des propriétés suivantes:*

(1) *toutes deux classes résiduelles soit coïncident, soit sont disjointes*;

(2) *la réunion de toutes les classes résiduelles de l'anneau $\mathcal{K}$ suivant l'idéal I coïncide avec l'ensemble* $|\mathcal{K}|$;

(3) *les classes résiduelles* $\bar{a}$ *et* $\bar{b}$ *suivant l'idéal I coïncident si et seulement si* $a \equiv b \pmod{I}$;

(4) *si* $c \in \bar{a}$, *alors* $\bar{a} = c + I$ (*en particulier*, $\bar{a} = a + I$).

Les propriétés (1)-(4) du théorème expriment les propriétés correspondantes des classes du groupe $\langle K, +, -\rangle$ suivant le sous-groupe $\langle I, +, -\rangle$.

Etudions les principales propriétés des congruences suivant un idéal.

PROPRIÉTÉ 1.1. *Les congruences peuvent être additionnées et soustraites membre à membre, c'est-à-dire de*

$$a \equiv b \quad \text{et} \quad c \equiv d \pmod{I}$$

s'ensuit

$$a + c \equiv b + d \quad \text{et} \quad a - c \equiv b - d \pmod{I}.$$

D é m o n s t r a t i o n. En effet, si $a - b \in I$ et $c - d \in I$, alors

$$a + c - (b + d) \in I \quad \text{et} \quad (a - c) - (b - d) \in I.$$

Par conséquent, $a + c \equiv b + d$, $a - c \equiv b - d \pmod{I}$. □

PROPRIÉTÉ 1.2. *Les deux membres de la congruence peuvent être multipliés par tout entier n, c'est-à-dire de* $a \equiv b \pmod{I}$ *il s'ensuit que* $na \equiv nb \pmod{I}$, *où* $n \in \mathbf{Z}$.

D é m o n s t r a t i o n. De $a - b \in I$ il s'ensuit que $na - nb = n(a - b) \in I$. □

PROPRIÉTÉ 1.3. *Les deux membres de la congruence peuvent être multipliés à droite et à gauche par tout élément de l'anneau, c'est-à-dire*

de

$$a \equiv b \pmod{I} \quad et \quad c \in |\mathscr{K}|$$

s'ensuivent les congruences

$$ca \equiv cb \pmod{I}, \qquad ac \equiv bc \pmod{I}.$$

D é m o n s t r a t i o n. L'ensemble des éléments de l'idéal I est stable par rapport à la multiplication par les éléments de l'anneau. Donc, pour tout élément c de l'anneau $\mathscr{K}$ de $a - b \in I$ s'ensuit $ca - cb \in I$ et $ac - bc \in I$. □

PROPRIÉTÉ 1.4. *Les congruences peuvent être multipliées membre à membre, c'est-à-dire si*

$$a \equiv b, \quad c \equiv d \pmod{I}, \text{ alors } ac \equiv bd \pmod{I}.$$

D é m o n s t r a t i o n. De fait, si $a - b \in I$ et $c - d \in I$, alors, en vertu de la stabilité de l'idéal I par rapport à l'addition et à la multiplication par les éléments de l'anneau, il vient

$$ac - bd = ac - bc + bc - bd = (a - b)\,c + b\,(c - d) \in I. \ \square$$

Anneau quotient. Soit I un idéal de l'anneau $\mathscr{K} = \langle K, +, -, \cdot, 1\rangle$. On a établi plus haut que la congruence modulo I est une relation d'équivalence sur l'ensemble K. Les classes d'équivalence sont appelées *classes résiduelles* ou *classes de l'anneau* $\mathscr{K}$ *suivant l'idéal* I *ou modulo* I. L'ensemble de toutes les classes résiduelles est dénommé *ensemble quotient* K *modulo* I et noté K/I.

Les propriétés 1.1-1.4 des congruences suivant l'idéal montrent que la congruence modulo I est une congruence dans l'anneau $\mathscr{K}$ (une congruence relativement à toutes les opérations principales de l'anneau $\mathscr{K}$). Aussi, selon le théorème 3.1.9, est-on en mesure de définir les opérations $+$, $-$, $\cdot$, $\bar{1}$ associées aux opérations principales de l'anneau $\mathscr{K}$ sur l'ensemble quotient K/I de la façon suivante:

$$\bar{a} + \bar{b} = \overline{a + b}, \quad -\bar{a} = \overline{(-a)}, \quad \bar{a}\bar{b} = \overline{ab}, \quad \bar{1} = 1 + I$$

pour tous éléments $\bar{a}$, $\bar{b}$ de K/I.

Une telle définition des opérations sur l'ensemble quotient K/I est correcte, car elle ne dépend pas du choix des éléments a, b dans les classes $\bar{a}$ et $\bar{b}$ respectivement.

DÉFINITION. L'algèbre $\langle K/I, +, -, \cdot, \bar{1}\rangle$ est dénommée *anneau quotient de l'anneau* $\mathscr{K}$ *modulo* I et notée $\mathscr{K}/I$.

THÉORÈME 1.3. *Soit* I *l'idéal de l'anneau* $\mathscr{K}$. *Dans ce cas l'algèbre* $\mathscr{K}/I = \langle K/I, +, -, \cdot, \bar{1}\rangle$ *est un anneau.*

D é m o n s t r a t i o n. L'algèbre $\langle K/I, +, -\rangle$ est un groupe abélien puisque c'est un groupe quotient du groupe additif $\langle K, +, -\rangle$ de l'anneau $\mathscr{K}$ suivant le sous-groupe $\langle I, +, -\rangle$ (voir théorème 10.4.2).

L'algèbre $\langle K/I, \cdot, \bar{1}\rangle$ est un *monoïde*. En effet, en vertu de l'associativité de la multiplication dans $\mathscr{K}$ pour tous $\bar{a}, \bar{b}, \bar{c}$ de K/I, on a

$$\bar{a}\cdot(\bar{b}\cdot\bar{c}) = \bar{a}\cdot(\overline{bc}) = \overline{a\,(bc)} = \overline{(ab)\,c} = (\overline{ab})\cdot\bar{c} = (\bar{a}\cdot\bar{b})\cdot\bar{c},$$

autrement dit, la multiplication dans l'algèbre $\mathscr{K}/I$ est associative. De plus,

$$\bar{a}\cdot\bar{1} = \overline{a\cdot 1} = \bar{a} = \bar{1}\cdot\bar{a} \quad \text{pour tout } \bar{a} \text{ de } K/I,$$

c'est-à-dire $\bar{1}$ est un élément neutre par rapport à la multiplication dans l'algèbre $\mathscr{K}/I$.

Dans $\mathscr{K}/I$ la multiplication est distributive par rapport à l'addition. En effet, en vertu de la distributivité de la multiplication par rapport à l'addition dans l'anneau $\mathscr{K}$ pour tous $\bar{a}, \bar{b}, \bar{c}$ de $\mathscr{K}/I$, il vient

$$(\bar{a} + \bar{b})\cdot\bar{c} = \overline{a + b}\cdot\bar{c} = \overline{(a + b)\cdot c} = \overline{ac + bc} =$$
$$= \overline{ac} + \overline{bc} = \bar{a}\cdot\bar{c} + \bar{b}\cdot\bar{c}.$$

De façon analogue, on se convainc que $\bar{c}\,(\bar{a} + \bar{b}) = \bar{c}\cdot\bar{a} + \bar{c}\cdot\bar{b}$. □

Théorème des épimorphismes d'anneaux. Soient $\mathscr{K}$ et $\mathscr{K}'$ des anneaux :

$$\mathscr{K} = \langle K, +, -, \cdot, 1\rangle, \qquad \mathscr{K}' = \langle K', +, -, \cdot, 1'\rangle.$$

THÉORÈME 1.4. *Un noyau d'homomorphisme de l'anneau $\mathscr{K}$ dans l'anneau $\mathscr{K}'$ est un idéal de l'anneau $\mathscr{K}$.*

D é m o n s t r a t i o n. Soit Ker f un noyau d'homomorphisme f de l'anneau $\mathscr{K}$ dans l'anneau $\mathscr{K}'$, c'est-à-dire Ker $f =$ $= \{x \in \mathscr{K} \mid f(x) = 0'\}$, où $0'$ est le zéro de l'anneau $\mathscr{K}'$. L'ensemble Ker f n'est pas vide, car $0 \in$ Ker f. Pour tous a, b de Ker f, il vient

$$f(a - b) = f(a) - f(b) = 0' - 0' = 0',$$

c'est-à-dire l'ensemble Ker f est fermé dans $\mathscr{K}$ par rapport à la soustraction.

Pour tout a de Ker f et tout k de K, il vient

$$f(ka) = f(k)\cdot f(a) = f(k)\cdot 0' = 0',$$

c'est-à-dire $ka \in$ Ker f. De façon analogue, on se convainc que $ak \in$ $\in$ Ker f.

Ainsi, Ker f est stable par rapport à la multiplication par les éléments de K. Par conséquent, le noyau d'homomorphisme f est un idéal de l'anneau $\mathscr{K}$. □

PROPOSITION 1.5. *Soit f un homomorphisme de l'anneau $\mathscr{K}$ dans l'anneau $\mathscr{K}'$ de noyau I. Pour tous a, b de K l'égalité $f(a) = f(b)$ est vérifiée si et seulement si $\bar{a} = \bar{b}$.*

D é m o n s t r a t i o n. Soit $f(a) = f(b)$. Alors,

(1) $f(a - b) = f(a) - f(b) = 0'$,

puisque f est un homomorphisme. Donc $a - b \in I$ et, par suite, $\bar{a} = \bar{b}$.

Admettons à présent que $\bar{a} = \bar{b}$. Alors, $a - b \in I$ et $f(a - b) = 0'$, vu que $I = \mathrm{Ker}\, f$. De là, compte tenu de (1), on obtient

$$f(a) - f(b) = 0' \quad \text{et} \quad f(a) = f(b). \ \square$$

THÉORÈME 1.6. *Soit f un épimorphisme de l'anneau $\mathscr{K}$ sur l'anneau $\mathscr{K}'$ de noyau I. Alors l'anneau quotient $\mathscr{K}/I$ est isomorphe à l'anneau $\mathscr{K}'$.*

D é m o n s t r a t i o n. Par hypothèse, $I = \mathrm{Ker}\, f$. Soit $\bar{K} = K/I$ l'ensemble de toutes les classes résiduelles de l'anneau $\mathscr{K}$ modulo I et

$$\mathscr{K}/I = \langle K/I, +, -, \cdot, \bar{1} \rangle,$$

où $\bar{1} = 1 + I$. Désignons par h l'application K/I dans $|\mathscr{K}'|$, qu'on définit de la façon suivante:

(1) $h(\bar{a}) = f(\bar{a})$ pour chaque élément $\bar{a}$ de K.

En vertu de la proposition 1.5, la valeur de $h(\bar{a})$ est indépendante du choix du représentant a dans la classe $\bar{a}$. Ensuite, l'application h respecte les opérations principales de l'anneau $\mathscr{K}/I$. En effet, $h(\bar{1}) = 1_{\mathscr{K}'}$ et pour tous $\bar{a}$, $\bar{b}$ de K, il vient:

$$h(\bar{a} + \bar{b}) = h(\overline{a + b}) = f(a + b) = f(a) + f(b) = h(\bar{a}) + h(\bar{b});$$
$$h(-\bar{a}) = h(\overline{(-a)}) = f(-a) = -f(a) = -h(\bar{a});$$
$$h(\bar{a} \cdot \bar{b}) = h(\overline{ab}) = f(ab) = f(a) \cdot f(b) = h(\bar{a}) \cdot h(\bar{b}).$$

Par hypothèse, f est une application de $|\mathscr{K}|$ sur $|\mathscr{K}'|$. En vertu de (1), il s'ensuit que h est une application de l'ensemble K sur l'ensemble $|\mathscr{K}'|$. L'application h est injective. De fait, en vertu de (1), de l'égalité $h(\bar{a}) = h(\bar{b})$ s'ensuit $f(a) = f(b)$; en vertu de la proposition 1.5, il en découle que $\bar{a} = \bar{b}$. Par conséquent, h est un isomorphisme de l'anneau quotient $\mathscr{K}/I$ sur l'anneau $\mathscr{K}'$. $\square$

Caractéristique d'un anneau. Soit $\mathscr{K} = \langle K, +, -, \cdot, e \rangle$ un anneau avec unité e. Dans le groupe additif $\langle K, +, - \rangle$ de l'anneau l'élément e est doué soit d'un ordre fini $\Theta(e) = m$, soit d'un ordre infini $\Theta(e) = \infty$.

DÉFINITION. On dit que l'anneau $\mathscr{K}$ possède une *caractéristique finie m* si dans le groupe additif de l'anneau l'unité de l'anneau a un ordre fini m. On dit que l'anneau $\mathscr{K}$ a une *caractéristique nulle* si l'unité de l'anneau $\mathscr{K}$ est douée d'un ordre infini.

Puisque tout corps $\mathscr{F}$ est un anneau, on peut parler de la caractéristique d'un corps $\mathscr{F}$. Convenons de noter $ch(\mathscr{K})$ la caractéristique de l'anneau $\mathscr{K}$.

Exemples. 1. Soit $\mathfrak{Z}$ un anneau des entiers. Pour tout entier positif n, on a la condition $n \cdot 1 \neq 0$, c'est-à-dire $\mathcal{O}(1) = \infty$. Par conséquent, un anneau des entiers a une caractéristique nulle.

2. Soit m un nombre naturel quelconque différent de zéro. L'anneau quotient $\mathfrak{Z}_m = \mathfrak{Z}/(m)$ admet une caractéristique finie m, vu que $\bar{1}$, unité de l'anneau $\mathfrak{Z}_m$, possède l'ordre m.

3. Soit $\mathscr{K}$ tout anneau numérique. Alors, pour tout entier positif n est satisfaite l'inégalité $n \cdot 1 \neq 0$ et, par suite, $\mathcal{O}(1) = \infty$. Donc, tout anneau numérique est de caractéristique nulle.

4. Soient $\mathscr{F}$ un corps de caractéristique m, $\mathscr{K}$ un anneau des matrices carrées sur $\mathscr{F}$ et E une matrice unité (unité de l'anneau). L'anneau $\mathscr{K}$ a la caractéristique m, car $\mathcal{O}(E) = \mathcal{O}(1_{\mathscr{F}}) = m$.

Théorème 1.7. *La caractéristique d'un domaine d'intégrité est soit zéro, soit un nombre premier.*

Démonstration. Soit $\mathscr{K}$ un domaine d'intégrité et e l'unité de l'anneau $\mathscr{K}$. Si $\mathcal{O}(e) = \infty$, alors $\mathscr{K}$ est de caractéristique nulle.

Si $\mathcal{O}(e) = 1$, alors $e = 1_{\mathscr{K}} = 0_{\mathscr{K}}$. Or, $1_{\mathscr{K}} \neq 0_{\mathscr{K}}$, vu que $\mathscr{K}$ est un domaine d'intégrité. Donc, $\mathcal{O}(e) \neq 1$.

Admettons maintenant que $\mathcal{O}(e) = m$ est un nombre composé naturel positif: $m = st$, $1 < s$, $t < m$. Par conséquent,

$$0 = m \cdot e = (st) \cdot e = (se) \cdot (t \cdot e).$$

Comme $\mathcal{O}(e) = m$ et $1 < s$, $t < m$, on a $s \cdot e \neq 0$ et $t \cdot e \neq 0$, mais puisque $\mathscr{K}$ est un domaine d'intégrité, il s'ensuit que $(s \cdot e) \cdot (t \cdot e) = m \cdot e \neq 0$. On a abouti à une contradiction en admettant que m est un nombre composé. Donc, m est un nombre premier. □

Théorème 1.8. *Soit p un élément premier de l'anneau $\mathfrak{Z}$. Alors l'anneau quotient $\mathfrak{Z}_p = \mathfrak{Z}/(p)$ est un corps.*

Démonstration. Soit $\bar{a}$ tout élément non nul de l'anneau $\mathfrak{Z}_p$. Il s'agit de démontrer que $\bar{a}$ est inversible dans l'anneau $\mathfrak{Z}_p$. La condition $\bar{a} \neq \bar{0}$ traduit le fait que p ne divise pas a. Donc, p et a sont premiers entre eux. Il existe donc des entiers m et n tels que $mp + na = 1$. Par conséquent, $\bar{n} \cdot \bar{a} = \bar{1}$, c'est-à-dire que l'élément $\bar{a}$ est inversible dans l'anneau $\mathfrak{Z}_p$. Ainsi, l'anneau $\mathfrak{Z}_p$ est un corps. □

Le plus petit sous-anneau d'un anneau. Le sous-anneau engendré par l'unité de l'anneau $\mathscr{K}$ est contenu dans tout sous-anneau de cet anneau.

Définition. Un sous-anneau de l'anneau $\mathscr{K}$ engendré par son unité est nommé *le plus petit* ou *le sous-anneau principal de l'anneau* $\mathscr{K}$.

Soient e l'unité de l'anneau $\mathscr{K} = \langle K, +, -, \cdot, e \rangle$, $E = \{ne \mid n \in \mathbf{Z}\}$ et $\mathscr{E}$ le plus petit sous-anneau de l'anneau $\mathscr{K}$. E est alors l'ensemble de base de l'anneau $\mathscr{E}$: $\mathscr{E} = \langle E, +, -, \cdot, e \rangle$. On vérifie sans peine que l'anneau $\mathscr{E}$ est une intersection de tous les sous-anneaux de l'anneau $\mathscr{K}$.

THÉORÈME 1.9. *Soit m la caractéristique de l'anneau $\mathcal{K}$ et $\mathcal{E}$ le plus petit sous-anneau de cet anneau. Si $m = 0$, alors $\mathcal{E}$ est isomorphe à l'anneau $\mathfrak{Z}$ des entiers. Si, par contre, $m > 0$, alors $\mathcal{E}$ est isomorphe à l'anneau quotient $\mathfrak{Z}/(m)$.*

Démonstration. Considérons l'application h de l'ensemble $\mathbf{Z}$ dans E telle que

(1) $h(n) = ne$ pour tout entier n.

En vertu de (1), h est une application de l'ensemble $\mathbf{Z}$ sur E et, de plus, h respecte les opérations principales de l'anneau $\mathfrak{Z}$, c'est-à-dire

$$h(n+s) = h(n) + h(s), \qquad h(-n) = -h(n),$$

$$h(n \cdot s) = h(n) \cdot h(s), \qquad h(1) = e$$

pour tous entiers n et s. Donc, h est un épimorphisme de l'anneau $\mathfrak{Z}$ sur l'anneau $\mathcal{E}$.

Montrons que $\operatorname{Ker} h = (m)$. En effet, puisque $h(m) = me = 0$, on a $(m) \subset \operatorname{Ker} h$. Ensuite, si $s \in \operatorname{Ker} h$, alors $h(s) = 0$ et, par suite, $s \cdot e = 0$. En outre, puisque $\Theta(e) = m$, on a $s \in (m)$, en vertu du théorème 10.3.1. Ainsi, $\operatorname{Ker} h \subset (m)$; par conséquent, $\operatorname{Ker} h = (m)$.

Selon le théorème d'épimorphismes d'un anneau, $\mathfrak{Z}/\operatorname{Ker} h \cong \mathcal{E}$. Mais puisque $\operatorname{Ker} h = (m)$, $\mathcal{E} \cong \mathfrak{Z}/(m)$. En particulier, $\mathcal{E} \cong \mathfrak{Z}/(0)$ pour $m = 0$. Par conséquent, pour $m = 0$ l'anneau $\mathcal{E}$ est isomorphe à l'anneau $\mathfrak{Z}$ des entiers. □

COROLLAIRE 1.10. *Soit $\mathcal{K}$ un domaine d'intégrité de caractéristique $m > 0$. Alors $\mathcal{E}$, le plus petit sous-anneau de l'anneau $\mathcal{K}$, est un corps.*

Démonstration. Puisque $m > 0$, alors selon le théorème 1.7, m est premier. Par conséquent, selon le théorème 12.3.7, $\mathfrak{Z}/(m)$ est un corps. En vertu du théorème 1.9, l'anneau $\mathcal{E}$ est isomorphe au corps $\mathfrak{Z}/(m)$ et, par suite, est lui-même un corps. □

Exercices

1. Soient n un entier quelconque et $n\mathbf{Z} = \{nx, x \in \mathbf{Z}\}$. Montrer que pour tout n l'ensemble $n\mathbf{Z}$ est un idéal de l'anneau $\mathfrak{Z}$. Montrer que tout idéal de l'anneau $\mathfrak{Z}$ est un ensemble $n\mathbf{Z}$ pour un certain nombre naturel n.
2. Montrer que des opérations binaires d'intersection et des sommes d'idéaux sont commutatives et associatives.
3. Démontrer que l'intersection d'idéaux à gauche (à droite) de l'anneau est un idéal à gauche (à droite) de l'anneau.
4. Montrer qu'un corps n'a pas d'idéaux autres que l'idéal nul et l'idéal unité.
5. Soit $\mathcal{V}$ un espace vectoriel de dimension finie sur le corps $\mathcal{F}$. Soit $\mathcal{K}$ un anneau d'opérateurs linéaires de l'espace $\mathcal{V}$. Démontrer que l'anneau $\mathcal{K}$ est démuni d'idéaux bilatères différents des idéaux nul et unité.
6. Chercher tous les idéaux de l'anneau $\mathfrak{Z}_{12}$.
7. Démontrer qu'un domaine d'intégrité fini est un corps.

8. Soient $\mathscr{K}$ un anneau et n un entier. Montrer que l'ensemble $\{x \in K \mid nx = 0_{\mathscr{K}}\}$ est un idéal de l'anneau $\mathscr{K}$.

9. Soit $\mathscr{F}$ un corps fini composé de m éléments. Démontrer que $a^m = a$ pour tout élément a du corps $\mathscr{F}$.

10. Chercher tous les automorphismes d'un corps des nombres complexes dont les nombres réels demeurent invariants.

11. Démontrer que pour tout isomorphisme des corps numériques le sous-corps des nombres rationnels constitue une application identique.

12. Démontrer que l'anneau des matrices de la forme

$$\begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix}$$

à a, b, c, d réels est isomorphe au corps (à l'anneau à division) des quaternions $a + bi + cj + dk$ sur le corps des nombres réels.

13. Démontrer que le plus petit sous-corps de tout corps de caractéristique nulle est isomorphe au corps des nombres rationnels.

14. Démontrer que $\mathfrak{Z}_6/2\mathbf{Z}_6 \cong \mathfrak{Z}_2$ et $\mathfrak{Z}_6/3\mathbf{Z}_6 \cong \mathfrak{Z}_3$.

15. Soit n un diviseur positif du nombre naturel m. Démontrer que $\mathfrak{Z}_m/n\mathbf{Z}_m \cong \mathfrak{Z}_n$.

16. Démontrer que le domaine de l'intégrité ne contenant que trois éléments est isomorphe à l'anneau quotient $\mathfrak{Z}/3\mathbf{Z}$.

17. Démontrer que les corps $\mathfrak{Q}(\sqrt{7})$ et $\mathfrak{Q}(\sqrt{11})$ ne sont pas isomorphes.

§ 2. Corps des quotients d'un domaine d'intégrité

Corps des quotients d'un domaine d'intégrité. Le problème de possibilité d'immersion d'un domaine d'intégrité dans un corps est d'importance majeure.

Définition. Un corps $\mathscr{F}$ est appelé *corps des quotients d'un domaine d'intégrité* $\mathscr{K}$ si sont remplies les conditions:

(α) $\mathscr{K}$ est un sous-anneau du corps $\mathscr{F}$;

(β) pour tout x de F il existe dans K des éléments a et b tels que $x = a \cdot b^{-1}$.

Théorème 2.1. *Pour tout domaine d'intégrité il existe un corps des quotients.*

Démonstration. Soient $\mathscr{K} = \langle K, +, -, \cdot, 1\rangle$ un domaine d'intégrité, $K^* = K \setminus \{0\}$ et

$$K \times K^* = \{\langle a, b\rangle \mid a \in K, \quad b \in K^*\}.$$

Définissons sur l'ensemble $K \times K^*$ la relation binaire $\equiv$ de la façon suivante:

$$\langle a, b\rangle \equiv \langle c, d\rangle \text{ si et seulement si } ad = bc.$$

Appelons *congruence sur* $K \times K^*$ cette relation. La congruence est réflexive, symétrique et transitive.

La réflexivité et la symétrie sont évidentes. La transitivité se manifeste également. En effet, il s'ensuit des prémisses que $ad = bc$, $cf = de$, $d \neq 0$. En multipliant les deux membres de la première

égalité par f, et de la seconde par b, on obtient: $adf = bcf$, $bcf = bed$ et, par suite, $adf = bed$. Cette dernière égalité implique $af = be$, vu que $\mathcal{K}$ est un domaine d'intégrité et $d \neq 0$. Donc, $\langle a, b\rangle \equiv \langle e, f\rangle$.

Ainsi, la congruence est une relation d'équivalence sur l'ensemble $K \times K^*$. La classe d'équivalence contenant le couple $\langle a, b\rangle$ est notée $[a, b]$, l'ensemble quotient $K \times K^*/\equiv$ par F_1. Remarquons que pour tous $[a, b]$ et $[c, d]$ de F_1, on a

(1) $[a, b] = [c, d]$ si et seulement si $ad = bc$.

Définissons sur l'ensemble $K \times K^*$ les opérations $\oplus$, $\ominus$, $\odot$:

$\langle a, b\rangle \oplus \langle c, d\rangle = \langle ad + bc, bd\rangle$;

$\ominus \langle a, b\rangle = \langle -a, b\rangle$;

$\langle a, b\rangle \odot \langle c, d\rangle = \langle ac, bd\rangle$.

$\mathcal{K}$ étant un domaine d'intégrité, $b \neq 0$ et $d \neq 0$ impliquent que $bd \neq 0$. Donc, l'ensemble $K \times K^*$ est fermé relativement aux opérations $\oplus$, $\ominus$ et $\odot$. On voit sans peine que les opérations d'addition et de multiplication sont commutatives.

Démontrons que la congruence sur $K \times K^*$ est une congruence pour les opérations $\oplus$, $\ominus$, et $\odot$. Compte tenu de ce que les opérations d'addition et de multiplication sont commutatives, il suffit de montrer que de la condition

(2) $\langle a, b\rangle \equiv \langle a', b'\rangle$

s'ensuivent les relations:

(3) $\langle a, b\rangle \oplus \langle c, d\rangle \equiv \langle a', b'\rangle \oplus \langle c, d\rangle$;

(4) $\ominus \langle a, b\rangle \equiv \ominus \langle a', b'\rangle$;

(5) $\langle a, b\rangle \odot \langle c, d\rangle \equiv \langle a', b'\rangle \odot \langle c, d\rangle$.

La vérification de (3) se ramène à l'établissement de la relation

$$\langle ad + bc, bd\rangle \equiv \langle a'd + b'c, b'd\rangle.$$

Cette relation se réduit à l'égalité

$$(ad + bc)\, b'd = (a'd + b'c)\, bd$$

qui, à son tour, peut être remplacée par l'égalité $ab'd^2 = a'bd^2$, qu'on obtient à partir de l'égalité $ab' = a'b$. Cette dernière égalité se déduit de la condition (2).

La vérification de (4) se ramène à l'établissement de la relation

$$\langle -a, b\rangle \equiv \langle -a', b'\rangle,$$

réduite à l'égalité $(-a)\, b' = (-a')\, b$ qui, à son tour, est remplacée par l'égalité $ab' = a'b$ valable en vertu de la condition (2).

La vérification de (5) se ramène à l'établissement de la relation

$$\langle ac,\ bd\rangle \equiv \langle a'c,\ b'd\rangle,$$

se réduisant à l'égalité $ac\cdot b'd = a'c\cdot bd$ qui, à son tour, est obtenue à partir de l'égalité $ab' = a'b$, vraie en vertu de la condition (2).

Bref, on a établi que la congruence sur l'ensemble $K \times K^*$ est une congruence pour les opérations $\oplus$, $\ominus$, $\odot$. Selon le théorème 3.1.9 sur les congruences, les *opérations* $+$, $-$, $.$ se définissent sur l'ensemble quotient F_1 au moyen des formules suivantes:

(6) $[a,\ b] + [c,\ d] = [ad + bc,\ bd]$;

(7) $-[a,\ b] = [-a,\ b]$;

(8) $[a,\ b]\cdot[c,\ d] = [ac,\ bd]$,

de plus, les valeurs des opérations définies ainsi sont indépendantes du choix arbitraire des couples $\langle a, b\rangle$ et $\langle c, d\rangle$ dans les classes d'équivalence $[a, b]$ et $[c, d]$ respectivement.

Pour tout élément a de K posons $\bar{a} = [a,\ 1]$, en particulier, $\bar{0} = [0,\ 1]$, $\bar{1} = [1,\ 1]$. Sur la base de (1) on conclut que:

$[a,\ b] = \bar{0}$ si et seulement si $a = 0$;

$[a,\ b] = \bar{1}$ si et seulement si $a = b$;

$[a,\ b] = [ac,\ bc]$ pour tout $c \neq 0$.

Démontrons que l'algèbre $\mathcal{F}_1 = \langle F_1,\ +,\ -,\ \cdot,\ \bar{1}\rangle$ est un *corps*. Une vérification directe montre que l'addition dans $\mathcal{F}_1$ est commutative et associative, $\bar{0}$ est un élément neutre par rapport à l'addition et, pour tout $[a,\ b]$ de F_1, il vient

$$[a,\ b] + (-[a,\ b]) = \bar{0}.$$

Par conséquent, l'algèbre $\langle F_1,\ +,\ -\rangle$ est un *groupe abélien*.

Une vérification directe montre également que la multiplication dans $\mathcal{F}_1$ est commutative et associative et $\bar{1}$ est un élément neutre par rapport à la multiplication. Donc, l'algèbre $\langle F_1,\ \cdot,\ \bar{1}\rangle$ est un *monoïde commutatif*.

Montrons que la multiplication dans $\mathcal{F}_1$ est distributive par rapport à l'addition, c'est-à-dire que pour tous $[a,\ b]$, $[c,\ d]$, $[e,\ f]$ de F_1, on a

$$([a,\ b] + [c,\ d])\ [e,\ f] = [a,\ b]\ [e,\ f] + [c,\ d]\ [e,\ f].$$

Il faut montrer que

$$[ade + bce,\ bdf] = [ae\cdot df + ce\cdot bf,\ bf\cdot df],$$

ou

$$\langle ade + bce,\ bdf\rangle \equiv \langle (ade + bce)\, f,\ bdf\cdot f\rangle \quad (f \neq 0).$$

La dernière relation est la conséquence de ce que $\langle a_1, b_1\rangle \equiv \langle a_1 f, b_1 f\rangle$ pour tous a_1, b_1, f avec $f \neq 0$.

Ainsi, l'algèbre $\mathcal{F}_1$ est un *anneau commutatif*. Dans l'anneau $\mathcal{F}_1$ est satisfaite la condition $\overline{0} \neq \overline{1}$, car $0 \cdot 1 \neq 1 \cdot 1$ dans le corps $\mathcal{F}$. Dans l'anneau $\mathcal{F}_1$ tout élément autre que $\overline{0}$ est inversible. En effet, si $[a, b] \neq \overline{0}$, alors $a \neq 0$, $[b, a] \in F_1$ et $[a, b]\cdot[b, a] = \overline{1}$. Bref, on a établi que l'algèbre $\mathcal{F}_1$ est un corps.

Le corps $\mathcal{F}_1$ contient un sous-anneau isomorphe à l'anneau $\mathcal{K}$. De fait, considérons l'ensemble $K_1 = \{[a, 1] \mid a \in K\}$. Cet ensemble est fermé dans $\mathcal{F}_1$, de sorte que

$$(9) \qquad [a, 1] + [b, 1] = [a + b, 1], \; -[a, 1] = [-a, 1], [a, 1]\,[b, 1] = \\ = [ab, 1], \; [1, 1] \in K_1$$

pour tous $[a, 1]$, $[b, 1]$ de K_1. Donc, l'algèbre $\mathcal{K}_1 = \langle K_1, +, -, \cdot, \overline{1}\rangle$ est un sous-anneau du corps $\mathcal{F}_1$. Définissons l'*application* h_1 *de l'ensemble* K_1 *dans* K de la façon suivante:

$$h_1([a, 1]) = a \text{ pour chaque } a \text{ de } K.$$

h_1 est apparemment une application injective de l'ensemble K_1 sur K. En vertu de (9), l'application h_1 respecte les opérations principales de l'anneau $\mathcal{K}_1$, c'est-à-dire

$$h_1(\overline{a} + \overline{b}) = a + b, \quad h_1(-\overline{a}) = -a, \quad h_1(\overline{ab}) = ab, \quad h_1(\overline{1}) = 1.$$

Ainsi, h_1 est un *isomorphisme de l'anneau* $\mathcal{K}_1$ sur l'anneau $\mathcal{K}$. Par conséquent, le corps $\mathcal{F}_1$ contient le sous-anneau $\mathcal{K}_1$ isomorphe à l'anneau de départ $\mathcal{K}$.

Il faut maintenant construire pour le corps $\mathcal{F}_1$ un nouveau corps isomorphe au corps $\mathcal{F}_1$ et contenant le sous-anneau $\mathcal{K}$. A cette fin, remplaçons dans l'ensemble F_1 chaque élément $[a, 1]$ par l'élément a (image de l'élément $[a, 1]$ après avoir fait opérer h_1), en laissant tous les autres éléments de l'ensemble F_1 inchangés. Posons $F = (F_1 \setminus K_1) \cup K$. Notons h l'application suivante de l'ensemble F_1 sur F:

$$h(x) = \begin{cases} h_1(x) & \text{si } x \in K_1, \\ x & \text{si } x \in F_1 \setminus K_1. \end{cases}$$

L'application h est une *application injective de l'ensemble* F_1 sur F prolongeant l'application h_1.

Définissons sur l'ensemble F les *opérations* $+$, $-$, $\cdot$ par les formules

$$(*) \qquad \begin{aligned} \alpha + \beta &= h(h^{-1}(\alpha) + h^{-1}(\beta)), \\ -\alpha &= h(-h^{-1}(\alpha)), \\ \alpha\cdot\beta &= h(h^{-1}(\alpha)\cdot h^{-1}(\beta)) \quad (\alpha, \beta \in F). \end{aligned}$$

Notons que $1 = h(\bar{1})$. Considérons l'algèbre $\mathcal{F} = \langle F, +, -, \cdot, 1\rangle$. Sur la base des formules (*) on conclut que les formules suivantes sont vraies:

$$h^{-1}(\alpha + \beta) = h^{-1}(\alpha) + h^{-1}(\beta),$$
$$h^{-1}(-\alpha) = -h^{-1}(\alpha) \quad (\alpha, \beta \in F),$$
$$h^{-1}(\alpha\beta) = h^{-1}(\alpha)\cdot h^{-1}(\beta),$$
$$h^{-1}(1) = \bar{1}.$$

Ces formules montrent que h^{-1} est un *isomorphisme de l'algèbre* $\mathcal{F}$ sur le corps $\mathcal{F}_1$. Par conséquent, l'algèbre $\mathcal{F}$ est un corps. Dans ce cas $\mathcal{K}$ est un sous-anneau du corps $\mathcal{F}$ car $K \subset F$ et, en vertu des formules (*), les opérations $+, -, \cdot$ dans $\mathcal{F}$ prolongent les opérations principales correspondantes de l'anneau $\mathcal{K}$. En effet, pour tous α, β de K, il vient:

$$\alpha + \beta = h([\alpha, 1] + [\beta, 1]) = h([\alpha + \beta, 1]) = \alpha + \beta;$$
$$-\alpha = h(-[\alpha, 1]) = h([-\alpha, 1]) = -\alpha;$$
$$\alpha\cdot\beta = h([\alpha, 1]\cdot[\beta, 1]) = h([\alpha\beta, 1]) = \alpha\beta.$$

Chaque élément x de F peut être représenté sous forme de quotient d'éléments de l'anneau $\mathcal{K}$. En effet, si $h^{-1}(x) = [a, b]$, où a, $b \in K$ et $b \neq 0$, alors

$$[a, b] = [a, 1]\cdot[1, b] \text{ et } h^{-1}(x) = \bar{a}\cdot(\bar{b})^{-1}.$$

Donc,

$$x = h(\bar{a}\cdot\bar{b}^{-1}) = h(\bar{a})\cdot h(\bar{b}^{-1}) = a\cdot b^{-1}, \text{ et, par suite, } x = a\cdot b^{-1}.$$

Bref, on a établi que $\mathcal{F}$ est un corps satisfaisant aux conditions: (α) $\mathcal{K}$ est un sous-anneau du corps $\mathcal{F}$; (β) pour tout x de F il existe dans K des éléments a, b tels que $x = a\cdot b^{-1}$. Par conséquent, $\mathcal{F}$ est un corps des quotients pour le domaine d'intégrité $\mathcal{K}$. □

Isomorphisme des corps des quotients. Montrons que tout domaine d'intégrité contient un corps unique des quotients à l'isomorphisme près.

THÉORÈME 2.2. *Soit* $\mathcal{K} = \langle K, +, -, \cdot, 1\rangle$ *un domaine d'intégrité. Soient* $\mathcal{F} = \langle F, +, -, \cdot, 1\rangle$ *et* $\mathcal{P} = \langle P, \oplus, \ominus, \odot, 1\rangle$ *des corps des quotients de l'anneau* $\mathcal{K}$. *Il existe alors un isomorphisme du corps* $\mathcal{F}$ *sur le corps* $\mathcal{P}$ *faisant passer chaque élément de l'anneau* $\mathcal{K}$ *dans lui-même.*

Démonstration. Par hypothèse, $\mathcal{F}$ est un corps des quotients, donc sont remplies les conditions:

(α) $\mathcal{K}$ est un sous-anneau du corps $\mathcal{F}$;

(β) pour tout x de F il existe dans K des éléments a, b tels que $x = a\cdot b^{-1}$. Ensuite, par hypothèse, $\mathcal{P}$ est un autre corps des quotients de l'anneau $\mathcal{K}$, donc, sont remplies les conditions:

(γ) $\mathscr{K}$ est un sous-anneau du corps $\mathscr{P}$;

(δ) pour tout y de P il existe dans K des éléments a_1, b_1 tels que $y = a_1 \odot b_1^{-1}$.

Définissons la *relation* h de la façon suivante:

(1) $h(a \cdot b^{-1}) = a \odot b^{-1}$ pour tous a, b de K.

Montrons que h est une application de F dans P. Il faut montrer que l'égalité (1) définit la seule valeur $h(x)$ qui ne dépend pas de la représentation concrète de l'élément x sous forme de $x = a \cdot b^{-1}$. En effet, si $x = c \cdot d^{-1}$ $(c, d \in K)$ est une autre représentation quelconque de cette forme de l'élément x, alors $a \cdot b^{-1} = c \cdot d^{-1}$. Donc, en vertu de (α) $a \cdot d = b \cdot c$. En vertu de (γ), il s'ensuit que $a \odot b^{-1} = c \odot b^{-1}$. Donc,

$$h(a \cdot b^{-1}) = a \odot b^{-1} = c \odot d^{-1} = h(c \cdot d^{-1}).$$

Ainsi, on a établi que h est une application (fonction). En vertu de (1) et de la condition (β) $\mathrm{Dom}\, h = F$. En vertu de (1) et de la condition (δ) $\mathrm{Im}\, h = P$. Par conséquent, h est une application de l'ensemble F sur P.

Une vérification directe montre que h est un homomorphisme du corps $\mathscr{F}$ sur le corps $\mathscr{P}$, c'est-à-dire pour tous x, y de F sont satisfaites les conditions

$$h(x + y) = h(x) \oplus h(y), \quad h(-x) = \ominus h(x),$$
$$h(x \cdot y)\, h(x) \odot h(y), \; h(1_{\mathscr{F}}) = 1_{\mathscr{P}}.$$

L'application h est injective. En effet, si pour des éléments $a \cdot b^{-1}$ et $c \cdot d^{-1}$ de F, on a

(2) $h(a \cdot b^{-1}) = h(c \cdot d^{-1})$,

alors, selon (1) dans le corps $\mathscr{P}$ se vérifie l'égalité $a \odot b^{-1} = c \odot d^{-1}$. En vertu de (δ), il s'ensuit l'égalité $a \cdot d = b \cdot c$. En vertu de (α) de la dernière égalité on déduit que

(3) $a \cdot b^{-1} = c \cdot d^{-1}$.

Bref, il a été établi que, pour tous éléments $a \cdot b^{-1}$ et $c \cdot d^{-1}$ de l'ensemble F, de (2) s'ensuit (3). h est donc une application injective. De plus, h est un homomorphisme. Par conséquent, h est un isomorphisme du corps $\mathscr{F}$ sur le corps $\mathscr{P}$. Enfin, en vertu de (1), $h(a) = a$ pour tout a de K, c'est-à-dire h fait passer chaque élément de l'anneau $\mathscr{K}$ dans lui-même. □

Exercices

1. Soient $\mathscr{K}$ un sous-anneau du corps $\mathscr{F}$ et K son ensemble de base. Soit $\mathscr{P}$ un sous-corps du corps $\mathscr{F}$ engendré par l'ensemble K, c'est-à-dire $\mathscr{P}$ est l'intersection de tous les sous-corps du corps $\mathscr{F}$ contenant l'ensemble K. Démontrer que $\mathscr{P}$ est un corps des quotients de l'anneau $\mathscr{K}$.

2. Soient $Z[i] = \{m + ni \mid m,\ n \in Z\}$ et $\mathscr{Z}[i]$ un sous-anneau du corps des nombres complexes avec ensemble de base $Z[i]$. Soient $\mathfrak{Q}(i) = \{a + bi \mid a,\ b \in Q\}$ et $\mathfrak{Q}(i)$ un sous-corps des nombres complexes à ensemble de base $Q(i)$. Montrer que $\mathfrak{Q}(i)$ est un corps des quotients de l'anneau $\mathscr{Z}[i]$.

3. Soient $\mathscr{P}$ et $\mathscr{P}'$ des corps des quotients des domaines d'intégrité $\mathscr{K}$ et $\mathscr{K}'$ respectivement et h un isomorphisme de $\mathscr{K}$ sur $\mathscr{K}'$. Démontrer qu'il existe un isomorphisme unique du corps $\mathscr{P}$ sur $\mathscr{P}'$ prolongeant l'isomorphisme h.

4. Soient $\mathscr{P}$ un corps des quotients du domaine d'intégrité $\mathscr{K}$ et φ un monomorphisme de $\mathscr{K}$ dans le corps $\mathscr{F}$. Démontrer que φ peut être prolongé et cela de façon unique jusqu'au monomorphisme du corps $\mathscr{P}$ dans le corps $\mathscr{F}$.

§ 3. Anneaux des idéaux principaux

Propriétés élémentaires de la divisibilité dans un anneau commutatif. Soient $\mathscr{K}$ un anneau commutatif et a, b ses éléments.

DÉFINITION. L'élément b est dit *diviseur de* a et l'élément a *multiple de* b s'il existe dans $\mathscr{K}$ un élément c tel que $a = bc$.

La notation $b \mid a$ traduit que b est un diviseur de a. La notation $a \vdots b$ témoigne que a est divisible par b ou bien que a est multiple de b.

L'élément c est appelé *diviseur commun* de a et b si $c \mid a$ et $c \mid b$ (ou $a \vdots c$ et $b \vdots c$). De façon analogue, est défini le diviseur commun de plusieurs éléments d'un anneau.

Les éléments a et b de l'anneau $\mathscr{K}$ sont dits *associés* dans $\mathscr{K}$ si $a \mid b$ et $b \mid a$.

L'élément a est dit *inversible* dans $\mathscr{K}$ ou *diviseur de l'unité* s'il existe dans $\mathscr{K}$ un élément b tel que $ab = 1$; dans ce cas on écrit $b = a^{-1}$.

Un diviseur de l'unité divise tout élément de l'anneau. Si $\mathscr{K}$ est un corps, alors tout élément de ce dernier est inversible s'il est différent de zéro.

Etudions les propriétés élémentaires de la divisibilité dans un anneau commutatif.

PROPOSITION 3.1. *La relation de divisibilité dans un anneau est réflexive et transitive, c'est-à-dire est une relation de préordre.*

PROPOSITION 3.2. *Un diviseur commun de deux ou plusieurs éléments d'un anneau est un diviseur de leur somme et de leur produit.*

PROPOSITION 3.3. *Si l'élément c divise un au moins des éléments $a_1, \ldots, a_n$, il divise alors le produit de ces éléments.*

PROPOSITION 3.4. *Une relation d'associativité dans un anneau commutatif est une relation d'équivalence.*

PROPOSITION 3.5. *Si a est associé à b et $b \mid c$, alors $a \mid c$.*

La démonstration des propositions 3.1-3.5 est laissée au soin du lecteur.

PROPOSITION 3.6. *Dans un domaine d'intégrité les éléments a et b sont associés si et seulement s'il existe un élément u inversible dans l'anneau tel que $a = ub$.*

D é m o n s t r a t i o n. Soient $\mathcal{K}$ un domaine d'intégrité et a, b des éléments associés dans $\mathcal{K}$, $a \sim b$. Si l'un des éléments a, b est nul, l'autre est obligatoirement égal à zéro. On a alors $a = 1_{\mathcal{K}} \cdot b$.

Supposons que $a \sim b$ et $a \neq 0$, $b \neq 0$. Il existe alors des éléments non nuls u et v tels que $a = ub$ et $b = va$. Donc, $a = uva$ et $a(uv - 1) = 0$. $\mathcal{K}$ étant un domaine d'intégrité et $a \neq 0$, il s'ensuit de la dernière égalité que $uv - 1 = 0$ et $uv = 1$. Ainsi, l'élément u est inversible dans $\mathcal{K}$ et $a = ub$.

Admettons à présent que $a = \varepsilon b$, où ε est un élément inversible de l'anneau $\mathcal{K}$; alors $b = \varepsilon^{-1}a$. Par conséquent, a et b sont associés dans $\mathcal{K}$. □

PROPOSITION 3.7. *Soit A l'ensemble de tous les éléments inversibles de l'anneau commutatif $\mathcal{K}$, $\mathcal{K} = \langle K, +, -, \cdot, 1\rangle$. Dans ce cas l'algèbre $\langle A, \cdot, ^{-1}\rangle$, où $^{-1}$ est une opération singulaire associant à l'élément a de A l'elément inverse a^{-1}, est un groupe.*

La démonstration de la proposition 3.7 est laissée au soin du lecteur.

Eléments simples et composés d'un domaine d'intégrité. Soit $\mathcal{K}$ un domaine d'intégrité. Tout élément a de l'anneau est divisible par tout élément inversible de l'anneau (par tout diviseur unité de l'anneau) ainsi que par chaque élément associé à a de l'anneau. Ces diviseurs sont dits *diviseurs triviaux de l'élément a.*

DEFINITION. On appelle *diviseur propre de l'élément a* tout diviseur non trivial de a, c'est-à-dire un diviseur non associé à a et irréversible dans l'anneau $\mathcal{K}$.

DEFINITION. Un élément du domaine d'intégrité $\mathcal{K}$ est dit *composé* ou *réductible dans* $\mathcal{K}$ s'il est différent de zéro et si l'on peut le représenter sous forme d'un produit de deux éléments irréversibles de l'anneau $\mathcal{K}$.

En d'autres termes, un élément du domaine d'intégrité est dit *composé* s'il est différent de zéro et s'il peut être représenté sous forme de produit de deux diviseurs propres.

DEFINITION. Un élément du domaine d'intégrité $\mathcal{K}$ est dit *simple* ou *irréductible* dans $\mathcal{K}$ s'il est différent de zéro, irréversible et n'admet que des diviseurs triviaux.

Notons que tout corps est démuni d'éléments simples comme d'éléments composés.

E x e m p l e s. 1. Dans un anneau $\mathfrak{Z}$ des entiers l'élément p différent de 0 et de ± 1 est un élément simple si et seulement si ses diviseurs ne sont que les éléments ± 1, $\pm p$. Dans l'anneau $\mathfrak{Z}$ les nombres ± 2, ± 3, ± 5, . . . sont simples (ou premiers).

2. Dans l'anneau $\mathfrak{Z}$, 6 est un élément composé, car $6 = 2 \cdot 3$ et 2, 3 sont des éléments irréversibles.

L'ensemble de tous les éléments d'un domaine d'intégrité se divise en quatre classes : 1) l'ensemble comportant un élément zéro ; 2) l'ensemble de tous les éléments inversibles (l'ensemble de tous les diviseurs unité) ; 3) l'ensemble de tous les éléments simples (pre-

miers); 4) l'ensemble de tous les éléments composés. Les deux dernières classes peuvent être vides (si le domaine d'intégrité est un corps).

THÉORÈME 3.8. *Soient $\mathcal{K}$ un domaine d'intégrité, a, $b \in K$ et 1 l'élément unité de l'anneau $\mathcal{K}$. Alors:*

(1) *$b \mid a$ si et seulement si $(a) \subset (b)$;*
(2) *$a \mid 1$ si et seulement si $(a) = (1)$;*
(3) *$a \sim b$ si et seulement si $(a) = (b)$;*
(4) *si b est un diviseur propre de a, alors $(a) \subsetneq (b)$;*
(5) *$a \subsetneq (b)$ si et seulement si $b \mid a$ et a ne divise pas b.*

D é m o n s t r a t i o n. (1) Soit $b \mid a$, c'est-à-dire qu'il existe un élément c de K tel que $a = bc$; alors $a \in (b)$;

$$(a) = \{ma \mid m \in K\} = \{mcb \mid m \in K\} \subset \{lb \mid l \in K\} = (b)$$

et, par suite, $(a) \subset (b)$. Admettons maintenant que $(a) \subset (b)$; alors $a \in (b)$ et, par suite, $a = bc$ pour un certain c de K, i.e. $b \mid a$;

(2) si $a \mid 1$, alors $(1) \subset (a)$, en vertu de (1). En outre, $(a) \subset (1)$, vu que $(1) = K$; donc, $(a) = (1)$. Si $(a) = (1)$, on a alors $a \mid 1$, en vertu de (1);

(3) si $a \sim b$, c'est-à-dire $a \mid b$ et $b \mid a$, alors, en vertu de (2), $(b) \subset (a)$ et $(a) \subset (b)$ et, par suite, $(a) = (b)$. Si $(a) = (b)$, alors $a \in (b)$ et $b \in (a)$, et donc, $b \mid a$ et $a \mid b$, par conséquent, $a \sim b$;

(4) supposons que b est un diviseur propre de a, c'est-à-dire $b \not\sim 1$, $b \not\sim a$ et $b \mid a$. Alors, en vertu de (1) et (3), $(b) \neq (a)$ et $(a) \subset (b)$, et, par suite, $(a) \subsetneq (b)$;

(5) si $(a) \subsetneq (b)$, alors, en vertu de (1), $b \mid a$ et, en vertu de (3), $a \not\sim b$ et, par suite, $b \nmid a$. La réciproque se déduit de (1) et (3). □

Anneaux des idéaux principaux. Il faut dégager et étudier dans la classe des domaines d'intégrité les anneaux dont chaque idéal soit principal.

DÉFINITION. On appelle *anneau d'idéaux principaux* ou *anneaux principaux* le domaine d'intégrité dont chaque idéal est l'idéal principal.

E x e m p l e s. 1. Tout corps est un anneau d'idéaux principaux.

2. L'anneau $\mathbb{Z}$ des entiers est un anneau d'idéaux principaux.

Rappelons que l'ensemble $(a, b) = \{ax + by \mid x, y \in K\}$, où a, b sont des éléments fixés de K, est un idéal d'un anneau commutatif $\mathcal{K}$.

Etudions les propriétés des anneaux d'idéaux principaux.

PROPOSITION 3.9. *Soient p un élément simple de l'anneau $\mathcal{K}$ des idéaux principaux et $a \in K$. Si p ne divise pas a, alors $(p, a) = (1)$.*

D é m o n s t r a t i o n. Par hypothèse, chaque idéal de l'anneau $\mathcal{K}$ est principal. Donc, il existe dans $\mathcal{K}$ un élément c tel que

$(p, a) = (c)$. L'élément c divise les éléments p et a:

(1) $c \mid p, \quad c \mid a$.

Vu que c est un diviseur de l'élément simple p, $c \sim p$ ou c divise 1. Si $c \sim p$, alors $p \mid c$ et puisqu'en vertu de (1) $c \mid a$, on a $p \mid a$, ce qui est en contradiction avec l'hypothèse. Donc, c divise 1. Par conséquent, $(c) = (1)$ et $(p, a) = (1)$. □

PROPOSITION 3.10. *Soient p un élément simple de l'anneau $\mathcal{K}$ d'idéaux principaux et $a, b \in K$. Si p divise ab, alors p divise également a ou b.*

Démonstration. Si p ne divise pas a, alors, en vertu de la proposition 3.9, $(p, a) = (1)$. Il existe donc dans K des éléments u, v tels que $up + va = 1$. En multipliant les deux membres de l'égalité par b, il vient $upb + vab = b$. Donc, si p divise ab, il divise également $upb + vab$ et b. Ainsi, si $p \nmid a$, alors $p \mid b$. □

PROPOSITION 3.11. *Soient p un élément simple de l'anneau $\mathcal{K}$ d'idéaux principaux et $a_1, \ldots, a_n \in K$. Si p divise le produit $a_1a_2 \ldots a_n$, alors il divise un au moins des facteurs $a_1, \ldots, a_n$.*

La démonstration de cette proposition s'effectue par récurrence sur n en s'appuyant sur la proposition 3.10.

DÉFINITION. La suite $(a_1), (a_2), (a_3), \ldots$ des idéaux principaux d'un anneau est appelée *chaîne ascendante des idéaux* si

(1) $(a_1) \subsetneqq (a_2) \subsetneqq (a_3) \subsetneqq \ldots$

PROPOSITION 3.12. *Dans un anneau d'idéaux principaux une chaîne ascendante des idéaux ne peut être infinie.*

Démonstration. Soit (1) la chaîne ascendante de l'anneau $\mathcal{K}$ d'idéaux principaux. Notons I la réunion de tous les idéaux de la chaîne (1), c'est-à-dire

(2) $I = \bigcup_i (a_i)$.

Une vérification directe montre que l'ensemble I est fermé par rapport à la soustraction et stable par rapport à la multiplication par les éléments de l'anneau $\mathcal{K}$. I est donc un idéal de l'anneau $\mathcal{K}$ et, de plus, un idéal principal. Il existe donc dans K un élément c tel que $I = (c)$. En nous appuyant sur (2) cherchons un indice m tel que $c \in (a_m)$. $c \in (a_m)$ et $a_m \in I = (c)$, on a $I = (a_m) = (c)$. Donc, l'idéal (a_m) est le dernier maillon de la chaîne (1). □

Anneau factoriel d'idéaux principaux. On se propose de généraliser aux anneaux d'idéaux principaux le théorème de l'existence et de l'unicité de la factorisation d'éléments de l'anneau $\mathbb{Z}$ des entiers.

DÉFINITION. On dit qu'un élément a du domaine d'intégrité $\mathcal{K}$ admet une factorisation unique si sont remplies les conditions suivantes:

(1) il existe dans $\mathcal{K}$ des éléments simples (premiers) p_i tels que $a = \prod_{i=1}^{m} p_i$;

(2) si $a = \prod_{i=1}^{n} q_i$ est une autre factorisation, où q_i sont des éléments simples de $\mathcal{K}$, alors $m = n$ et pour une numération adéquate $p_i \sim q_i$ pour $i = 1, \ldots, m$.

DÉFINITION. L'anneau $\mathcal{K}$ est dit *factoriel* (à factorisation unique) si c'est un domaine d'intégrité et tout élément de l'anneau différent de zéro et irréversible se décompose en facteurs premiers.

Notons que tout corps est un anneau factoriel vu qu'il ne possède pas d'éléments irréversibles différents de zéro.

THÉORÈME 3.13. *Un anneau d'idéaux principaux est un anneau factoriel.*

Démonstration. Soit $\mathcal{K}$ un anneau d'idéaux principaux. Il nous faut démontrer que tout élément irréversible différent de zéro de l'anneau se décompose en facteurs premiers. Supposons qu'il existe dans $\mathcal{K}$ un élément irréversible non nul a indécomposable en facteurs premiers dans $\mathcal{K}$. L'élément a est alors un élément composé. On peut donc le représenter sous forme d'un produit de deux diviseurs propres $a = a_1b_1$ et, selon le point (4) du théorème 3.8, $(a) \subsetneqq (a_1)$.

Un au moins des facteurs a_1, b_1, par exemple a_1, ne se décompose en facteurs premiers. On peut donc représenter a_1 sous forme de produit de deux facteurs propres:

$$a_1 = a_2b_2, \quad (a_1) \subsetneqq (a_2),$$

etc. Ainsi, il existe une chaîne ascendante infinie

$$(a) \subsetneqq (a_1) \subsetneqq (a_2) \subsetneqq \ldots$$

d'idéaux de l'anneau $\mathcal{K}$, ce qui est impossible en vertu de la proposition 3.12. Donc, tout élément irréversible différent de zéro de l'anneau $\mathcal{K}$ se décompose en facteurs premiers.

Démontrons que cette factorisation est unique. Si a est un élément simple, le théorème est alors vrai. Supposons que le théorème est vrai pour des éléments représentés sous forme de produit de n facteurs premiers et démontrons qu'il est aussi vrai pour des éléments représentables sous forme de produit de $n + 1$ facteurs premiers. Soient données deux décompositions quelconques de l'élément a en facteurs premiers:

(1) $\quad a = p_1 \cdot \ldots \cdot p_n p_{n+1} = q_1 \cdot \ldots \cdot q_s q_{s+1}.$

L'élément simple p_{n+1} divise le produit $q_1 \ldots q_{s+1}$. Par conséquent, selon la proposition 3.14, il divise un au moins des facteurs $q_1, \ldots, q_{s+1}$, par exemple q_{s+1}. p_{n+1} et q_{s+1} étant des nombres premiers,

on a $q_{s+1} = up_{n+1}$, où u est un élément inversible de l'anneau. En simplifiant les deux membres de l'égalité (1) par p_{n+1}, il vient

$$p_1 \ldots p_n = q_1 \ldots (uq_s).$$

Donc, par hypothèse de récurrence $n = s$ et pour une numération adéquate $p_i \sim q_i$ pour $i = 1, \ldots, n$. En outre, $p_{n+1} \sim q_{n+1}$. Le raisonnement par récurrence est achevé. □

Anneaux euclidiens. Soient N l'ensemble de tous les nombres naturels, K l'ensemble de base de l'anneau $\mathscr{K}$.

DÉFINITION. Un domaine d'intégrité $\mathscr{K}$ est dit *anneau euclidien* s'il existe une application h de l'ensemble K dans N satisfaisant aux conditions:

(α) pour tous a, b de K avec $b \neq 0$ il existe dans K des éléments q, r tels que $a = bq + r$ et $h(r) < h(b)$;

(β) pour tout a de K l'égalité $h(a) = 0$ est vraie si et seulement si $a = 0$.

Exemple. Soit h une application de l'ensemble **Z** des entiers dans N pour laquelle $h(a) = |a|$. En vertu du théorème de la division avec reste (voir théorème 4.4.4), h remplit les conditions (α) et (β). Donc, $\mathfrak{Z}$ est un anneau euclidien.

THÉORÈME 3.14. *Un anneau euclidien est un anneau d'idéaux principaux.*

Démonstration. Soient $\mathscr{K}$ un anneau euclidien et h l'application de l'ensemble K dans N satisfaisant aux conditions (α) et (β). L'idéal nul est apparemment l'idéal principal. Soit M un idéal non nul de l'anneau $\mathscr{K}$. Il nous faut démontrer que M est un idéal principal. Vu que $M \setminus \{0\}$ est un ensemble non vide, en vertu de (β), $h(M \setminus \{0\})$ est un sous-ensemble non vide de l'ensemble $\mathbf{N} \setminus \{0\}$ et, par suite, selon le théorème 4.3.11, $h(M \setminus \{0\})$ contient le plus petit élément. Par conséquent, il existe dans M un élément non nul b tel que

(1) $h(b) \leqslant h(x)$ pour tout x de $M \setminus \{0\}$.

Démontrons que $M = (b)$. Soit a un élément quelconque de l'ensemble $M \setminus \{0\}$. En vertu de la condition (α), il existe dans K des éléments q et r tels que

(2) $a = bq + r$ et $h(r) < h(b)$.

Vu que M est un idéal et $a, b \in M$, on a $r = a - bq \in M$ et, en vertu de (1), (2) il vient

(3) $r \notin M \setminus \{0\}$.

Donc, $r = 0$ et $a = bq$. Or, comme a est un élément non nul quelconque de l'ensemble M, $M \subset (b)$. Vu que $b \in M$, on a $M = (b)$; par conséquent, tout idéal de l'anneau euclidien $\mathscr{K}$ est un idéal principal. □

COROLLAIRE 3.15. *Tout anneau euclidien est un anneau factoriel.*

COROLLAIRE 3.16. *Un anneau $\mathfrak{Z}$ des entiers est un anneau des idéaux principaux et, partant, un anneau factoriel.*

Exemple. Soit $\mathbf{Z}[i] = \{m + ni \mid m, n \in \mathbf{Z}\}$. L'ensemble $\mathbf{Z}[i]$ est fermé dans l'anneau $\mathscr{C}$ des nombres complexes. Donc, l'algèbre $\mathfrak{Z}[i] = \langle \mathbf{Z}[i], +, -, \cdot, 1\rangle$ est un sous-anneau de l'anneau $\mathscr{C}$. Cet anneau est nommé *anneau des entiers gaussiens*. Montrons que l'anneau $\mathfrak{Z}[i]$ est euclidien. Considérons l'application h de l'ensemble $\mathbf{Z}[i]$ dans $\mathbf{N}$ pour laquelle, pour $a = m+ni$, $h(a) = |a|^2 = m^2 + n^2$. La condition (β) est apparemment remplie. Montrerons que pour h est remplie la condition (α). Soient $a, b \in \mathbf{Z}[i]$ et $b \neq 0$. Alors $a/b = \sigma + \tau i$, où $\sigma, \tau \in \mathbf{Q}$. Il existe des entiers s et t tels que $|s - \sigma| \leqslant \frac{1}{2}$ et $|t - \tau| \leqslant \frac{1}{2}$. Posons $\alpha = \sigma - s$ et $\beta = \tau - t$. Alors, $a = b(s + \alpha + (t + \beta)i) = bq + r$, où $q = s + ti$ et $r = b(\alpha + \beta i)$; de plus, $q = s + ti \in \mathbf{Z}[i]$ et $r = a - bq \in \mathbf{Z}[i]$. Donc, $h(r) = |r|^2 = |b|^2(\alpha^2 + \beta^2) \leqslant \frac{1}{2}|b|^2 = \frac{1}{2}h(b)$ et $h(r) < h(b)$, c'est-à-dire h satisfait également à la condition (α). Ainsi, l'anneau des entiers gaussiens est un anneau euclidien.

Exercices

1. Soient K un ensemble de tous les nombres rationnels m/n à dénominateurs impairs n et $\mathscr{K} = \langle K, +, -, \cdot, 1\rangle$ un sous-anneau du corps $\mathfrak{Q}$ des nombres rationnels. Montrer que $\mathscr{K}$ est un anneau d'idéaux principaux.

2. Soit $\mathfrak{Z}[i]$ un anneau des entiers gaussiens. Chercher les éléments inversibles de cet anneau.

3. Démontrer qu'un anneau quotient $\mathfrak{Z}[i]/(3)$ de l'anneau des entiers gaussiens suivant l'idéal (3) est un corps contenant neuf éléments.

4. Démontrer que l'anneau quotient $\mathfrak{Z}[i]/(n)$ de l'anneau des entiers gaussiens suivant l'idéal (n) est un corps si et seulement si n est un nombre premier non égal à la somme des carrés de deux entiers.

5. Soient $K = \{a + bi\sqrt{3} \mid a, b \in \mathbf{Z}\}$ et $\mathscr{K} = \langle K, +, -, \cdot, 1\rangle$ un sous-anneau d'un corps des nombres complexes. Montrer que dans l'anneau $\mathscr{K}$ tout élément irréversible différent de zéro se décompose en facteurs premiers, mais non pas toujours univoquement. En particulier, montrer que $4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ sont deux décompositions de 4 en produit de facteurs premiers, 2 n'étant pas associé à $1 \pm i\sqrt{3}$.

6. Soit K un ensemble de tous les nombres complexes de la forme $a + ib\sqrt{3}$, où a et b sont soit des entiers, soit tous les deux des moitiés d'entiers impairs. Soit $\mathscr{K}$ un sous-anneau d'un corps des nombres complexes à ensemble de base K. Démontrer que l'anneau $\mathscr{K}$ est euclidien.

7. Démontrer que l'élément p de l'anneau $\mathscr{K}$ d'idéaux principaux est simple (premier) si et seulement si l'anneau quotient $\mathscr{K}/(p)$ est un domaine d'intégrité.

8. Soient $\mathbf{Z}[\sqrt{2}] = \{m + n\sqrt{2} \mid m, n \in \mathbf{Z}\}$ et $\mathfrak{Z}[\sqrt{2}]$ un sous-anneau d'un corps des nombres réels à ensemble de base $\mathbf{Z}[\sqrt{2}]$. Démontrer que l'anneau $\mathfrak{Z}[\sqrt{2}]$ est euclidien.

§ 4. Plus grand commun diviseur. Plus petit commun multiple

Plus grand commun diviseur. Soit $\mathcal{K}$ un anneau commutatif. L'élément c est appelé *diviseur commun des éléments* $a_1, \ldots, a_m$ de l'anneau $\mathcal{K}$ si c est un diviseur (dans $\mathcal{K}$) de chacun de ces éléments.

DÉFINITION. On appelle *plus grand commun diviseur des éléments* $a_1, \ldots, a_m$ de l'anneau $\mathcal{K}$ leur plus grand commun diviseur divisible par tout commun diviseur de ces éléments.

Le plus grand commun diviseur des éléments $a_1, \ldots, a_n$ est noté PGCD $(a_1, \ldots, a_n)$.

De la définition susmentionnée découle la proposition suivante.

PROPOSITION 4.1. *Si d est le plus grand commun diviseur des éléments $a_1, \ldots, a_n$ dans $\mathcal{K}$, l'ensemble de tous les diviseurs communs des éléments $a_1, \ldots, a_n$ coïncide avec l'ensemble de tous les diviseurs de l'élément d.*

DÉFINITION. Les éléments a et b de l'anneau $\mathcal{K}$ sont dits *premiers entre eux* si l'unité (diviseur unité) de l'anneau $\mathcal{K}$ est leur plus grand commun diviseur dans $\mathcal{K}$.

On étudie plus bas les propriétés du plus grand commun diviseur dans l'anneau d'idéaux principaux. La proposition 4.2 est applicable à tout anneau commutatif.

PROPOSITION 4.2. *Tous deux plus grands communs diviseurs des éléments $a_1, \ldots, a_n$ de l'anneau $\mathcal{K}$ sont associés dans $\mathcal{K}$. Si c est le plus grand commun diviseur des éléments $a_1, \ldots, a_n$ tout en étant associé à d, alors d est également le plus grand commun diviseur de ces éléments.*

Cette propriété s'ensuit directement de la définition du plus grand commun diviseur.

PROPOSITION 4.3. *Pour toute collection d'éléments $a_1, \ldots, a_n$ de l'anneau $\mathcal{K}$ d'idéaux principaux il existe un plus grand commun diviseur dans $\mathcal{K}$. L'élément d est le plus grand commun diviseur des éléments $a_1, \ldots, a_n$ si et seulement si $(a_1, \ldots, a_n) = (d)$.*

D é m o n s t r a t i o n. Supposons que

$$(1) \quad (a_1, \ldots, a_n) = (d),$$

et démontrons que d est PGCD $(a_1, \ldots, a_n)$. Il s'ensuit de (1) que d est un commun diviseur des éléments $a_1, \ldots, a_n$ et on a :

$$(2) \quad d = \lambda_1 a_1 + \ldots + \lambda_n a_n, \text{ où } \lambda_1, \ldots, \lambda_n \in K.$$

En outre, en vertu de (2), si c est le diviseur commun de $a_1, \ldots, a_n$, alors c divise d. Donc, d est PGCD $(a_1, \ldots, a_n)$.

Posons maintenant que d est PGCD $(a_1, \ldots, a_n)$ et démontrons qu'alors $(a_1, \ldots, a_n) = (d)$. $\mathcal{K}$ étant l'anneau d'idéaux principaux, il existe dans K un élément c tel que $(a_1, \ldots, a_n) = (c)$. Comme on vient de le démontrer, c est PGCD $(a_1, \ldots, a_n)$. En vertu de la pro-

position 4.2, il s'ensuit que c et d sont associés et, par suite, selon le théorème 3.8, $(c) = (d)$. Par conséquent, $(a_1, \ldots, a_n) = (d)$. □

THÉORÈME 4.4. *Soit d le diviseur commun des éléments $a_1, \ldots, a_n$ de l'anneau $\mathcal{K}$ d'idéaux principaux. L'élément d est* PGCD $(a_1, \ldots, a_n)$ *si et seulement s'il peut être représenté sous forme de $d = \lambda_1 a_1 + \ldots + \lambda_n a_n$, où $\lambda_1, \ldots, \lambda_n \in K$.*

D é m o n s t r a t i o n. Soit d PGCD $(a_1, \ldots, a_n)$. Alors, selon la proposition 4.3, $(d) = (a_1, \ldots, a_n)$. On peut donc représenter d sous forme de $d = \lambda_1 a_1 + \ldots + \lambda_n a_n$, où $\lambda_1, \ldots, \lambda_n \in K$.

Posons maintenant que d peut être représenté sous forme de $d = \lambda_1 a_1 + \ldots + \lambda_n a_n$, $\lambda_i \in K$. Alors, tout diviseur commun c des éléments $a_1, \ldots, a_n$ divise la somme $\lambda_1 a_1 + \ldots + \lambda_n a_n$, et, partant, divise d. Par conséquent, d est le plus grand commun diviseur des éléments $a_1, \ldots, a_n$. □

PROPOSITION 4.5. *Pour tous éléments $a_1, \ldots, a_n$ et le diviseur commun c de l'anneau $\mathcal{K}$ d'idéaux principaux, on a*

$$\text{PGCD}\,(ca_1, \ldots, ca_n) \sim c\cdot\text{PGCD}\,(a_1, \ldots, a_n).$$

D é m o n s t r a t i o n. Soit d PGCD $(a_1, \ldots, a_n)$. Selon le théorème 4.4, il existe dans K des éléments $\lambda_1, \ldots, \lambda_n$ tels que $d = \lambda_1 a_1 + \ldots + \lambda_n a_n$. Donc $cd = \lambda_1 (ca_1) + \ldots + \lambda_n (ca_n)$. De plus, vu que d est le diviseur commun de $a_1, \ldots, a_n$, cd est aussi un diviseur commun de $ca_1, \ldots, ca_n$. Par conséquent, selon le théorème 4.4, cd est le plus grand commun diviseur des éléments $ca_1, \ldots, ca_n$. □

PROPOSITION 4.6. *Si d est le plus grand commun diviseur des éléments a et b dans l'anneau $\mathcal{K}$ d'idéaux principaux et $d \neq 0$ alors, les éléments a/d et b/d sont premiers entre eux.*

D é m o n s t r a t i o n. Par hypothèse, PGCD $(a, b) = d \neq 0$. Selon le théorème 4.4, il s'ensuit que $\lambda_1 a + \lambda_2 b = d$ pour certains $\lambda_1, \lambda_2 \in K$; aussi, $\lambda_1 \frac{a}{d} + \lambda_2 \frac{b}{d} = 1$. Selon le theorème 4.4, il s'ensuit que 1 est le plus grand commun diviseur des éléments a/d et b/d, et, partant, que les éléments a/d et b/d sont premiers entre eux. □

La proposition 4.6 peut apparemment être généralisée de la façon suivante: si d est le plus grand commun diviseur des éléments $a_1, \ldots, a_n$ dans l'anneau $\mathcal{K}$ d'idéaux principaux et $d \neq 0$, alors 1 est le plus grand commun diviseur des éléments $a_1/d, \ldots, a_n/d$.

THÉORÈME 4.7. *Si dans l'anneau d'idéaux principaux a divise bc et les éléments a, b sont premiers entre eux, alors a divise c.*

D é m o n s t r a t i o n. Par hypothèse, PGCD $(a, b) = 1$. Selon le théorème 4.4, il s'ensuit que $\lambda_1 a + \lambda_2 b = 1$ pour certains $\lambda_1, \lambda_2 \in K$. En multipliant les deux membres de l'égalité par c, on obtient $\lambda_1 ac + \lambda_2 bc = c$. Vu que, par hypothèse, a divise bc, il divise aussi $\lambda_1 ac + \lambda_2 bc$ et, partant, a divise c. □

Plus petit commun multiple. Soit $\mathscr{K}$ un anneau d'idéaux principaux. L'élément c est dit *multiple commun des éléments* $a_1, \ldots, a_n$ de l'anneau $\mathscr{K}$ si c se divise dans $\mathscr{K}$ par chacun de ces éléments.

DÉFINITION. On appelle *plus petit commun multiple des éléments* $a_1, \ldots, a_n$ de l'anneau $\mathscr{K}$ leur multiple commun qui divise tout multiple commun de ces éléments.

Un plus petit commun multiple des éléments $a_1, \ldots, a_n$ de l'anneau $\mathscr{K}$ est noté PPCM $(a_1, \ldots, a_n)$.

De cette définition s'ensuit directement la proposition suivante.

PROPOSITION 4.8. *Si m est le plus petit commun multiple des éléments $a_1, \ldots, a_n$ de l'anneau $\mathscr{K}$, l'ensemble de tous les multiples communs des éléments $a_1, \ldots, a_n$ coïncide alors avec l'ensemble de tous les multiples de l'élément m.*

Etudions les propriétés du plus petit commun multiple dans l'anneau $\mathscr{K}$ d'idéaux principaux. La proposition 4.9 s'applique à tout anneau commutatif.

PROPOSITION 4.9. *Tous deux plus petits communs multiples des éléments $a_1, \ldots, a_n$ de l'anneau $\mathscr{K}$ sont associés dans $\mathscr{K}$. Si m est le plus petit commun multiple des éléments $a_1, \ldots, a_n$ et m est associé à m', alors m' est aussi un plus petit commun multiple des éléments $a_1, \ldots, a_n$.*

Cette proposition découle directement de la définition du plus petit commun multiple.

PROPOSITION 4.10. *Un élément m est le plus petit commun multiple des éléments de l'anneau $\mathscr{K}$ si et seulement si*

$$(a_1) \cap (a_2) \cap \ldots \cap (a_n) = (m).$$

Démonstration. Supposons que

$$(a_1) \cap \ldots \cap (a_n) = (m). \tag{1}$$

Alors m est un multiple commun des éléments $a_1, \ldots, a_n$. En outre, si m' est un multiple commun des éléments $a_1, \ldots, a_n$, alors

$$m' \in (a_1), \ldots, m' \in (a_n), \text{ c'est-à-dire}$$
$$m' \in (a_1) \cap \ldots \cap (a_n) = (m)$$

et, partant, m' est multiple de m. Par conséquent, m est le plus petit commun multiple des éléments $a_1, \ldots, a_n$.

Supposons que m est PPCM $(a_1, \ldots, a_n)$. $\mathscr{K}$ étant un anneau d'idéaux principaux, il existe dans K un élément m_1 tel que

$$(a_1) \cap \ldots \cap (a_n) = (m_1).$$

Selon cette démonstration m_1 est le plus petit commun multiple des éléments $a_1, \ldots, a_n$. En raison de la proposition 4.9, m_1 est associé à m. Par conséquent,

$$(m_1) = (m) \text{ et } (a_1) \cap \ldots \cap (a_n) = (m). \quad \square$$

Corollaire 4.11. *Pour toute collection* $a_1, \ldots, a_n$ *d'éléments de l'anneau* $\mathscr{K}$ *il existe un plus petit commun multiple dans* $\mathscr{K}$.

Proposition 4.12. *Pour tous éléments* a, b, c *de l'anneau* $\mathscr{K}$

(1) $\text{PPCM}(ac, bc) \sim c \cdot \text{PPCM}(a, b)$.

Démonstration. Soit m PPCM (a, b). Il faut démontrer que mc est PPCM (ac, bc). C'est apparemment vrai pour $c = 0$. Supposons que $c \neq 0$. m étant un multiple commun de a et b, mc l'est de ac et bc. Soit m' tout multiple commun des éléments ac et bc, c'est-à-dire

(2) $m' = kac, \quad m' = sbc$, où $k, s \in K$.

Puisque $\mathscr{K}$ est un domaine d'intégrité et $c \neq 0$, de $kac = sbc$ il s'ensuit que $ka = sb$. Donc, ka est multiple de m, c'est-à-dire $ka = rm$, où $r \in K$. Par conséquent, en vertu de (2), $m' = rmc$ et, partant, m' est multiple de mc. Ainsi, mc est PPCM (ac, bc) et, selon la proposition 4.9, PPCM $(ac, bc) \sim cm$. □

Proposition 4.13. *Si a et b sont des éléments premiers entre eux de l'anneau* $\mathscr{K}$, *alors ab est un plus petit commun multiple des éléments a, b.*

Démonstration. Soit m un multiple commun quelconque de a et b. Démontrons que m est multiple de ab. Vu que m est un multiple de b, on a $m = bc$, où $c \in K$. Puisque a divise m et, par hypothèse, a et b sont premiers entre eux dans $\mathscr{K}$, a divise c (voir théorème 4.7). Donc, ab divise bc et, partant, m est multiple de ab. Par conséquent, ab est le plus petit commun multiple des éléments a, b. □

Proposition 4.14. *Si a, b sont des éléments non nuls de l'anneau* $\mathscr{K}$, *alors* $\text{PPCM}(a, b) \sim \dfrac{ab}{\text{PGCD}(a, b)}$.

Démonstration. Soit d PGCD (a, b) dans $\mathscr{K}$. Vu que a, b sont des éléments non nuls, on a $d \neq 0$. Selon la proposition 4.12,

(1) $\text{PPCM}(a, b) \sim d \cdot \text{PPCM}\left(\dfrac{a}{d}, \dfrac{b}{d}\right)$.

En vertu de la proposition 4.6, $\text{PGCD}\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$, c'est-à-dire les éléments $\dfrac{a}{d}$ et $\dfrac{b}{d}$ sont premiers entre eux. De là, selon la proposition 4.13, il s'ensuit que

(2) $\text{PPCM}\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = \dfrac{a}{d} \cdot \dfrac{b}{d}$.

Sur la base de (1) et (2) on conclut que $\text{PPCM}(a, b) \sim \dfrac{ab}{d}$. □

Théorème 4.15. *Soient* $a = u \cdot p_1^{\alpha_1} \ldots p_m^{\alpha_m}$, $b = v \cdot p_1^{\beta_1} \ldots p_m^{\beta_m}$, *où* $p_1, \ldots, p_m$ *sont des éléments irréversibles différents deux à deux de*

l'anneau factoriel $\mathscr{K}$, u, v étant des éléments inversibles de l'anneau. On a alors:

(1) $\text{PPCM}(a, b) = p_1^{\gamma_1} \dots p_m^{\gamma_m}$, *où* $\gamma_i = \max(\alpha_i, \beta_i)$;

(2) $\text{PGCD}(a, b) = p_1^{\delta_1} \dots p_m^{\delta_m}$, *où* $\delta_i = \min(\alpha_i, \beta_i)$.

La démonstration de la formule (1) s'esquisse de façon analogue à celle de la proposition 11.3.8. La démonstration de la formule (2) s'esquisse de la façon analogue à celle de la proposition 11.3.1.

Exercices

1. Démontrer le théorème 4.15.
2. Démontrer que le théorème 4.7 et la proposition 4.6 sont vrais pour tout anneau factoriel $\mathscr{K}$.
3. Montrer que les propositions 4.10-4.14 sont vraies pour tout anneau factoriel $\mathscr{K}$.
4. Soient a, b, c des éléments d'un anneau factoriel, PGCD $(a, c) \sim 1$ et PGCD $(b, c) \sim 1$. Démontrer que PGCD $(ab, c) \sim 1$.
5. Soient a, b, c des éléments d'un anneau factoriel. Démontrer que PPCM $(a$, PGCD $(b, c)) \sim$ PGCD (PPCM (a, b), PPCM $(a, c))$.

CHAPITRE XIV

POLYNÔMES À UNE VARIABLE

§ 1. Anneau des polynômes

Extension transcendante simple de l'anneau. Soient $\mathcal{K}$ et $\mathcal{L}$ des anneaux commutatifs à ensembles de base K et L respectivement.

DÉFINITION. Un anneau $\mathcal{L}$ est dit *extension simple de l'anneau* $\mathcal{K}$ par adjonction de l'élément u si sont satisfaites les conditions:

(1) $\mathcal{K}$ est un sous-anneau de l'anneau $\mathcal{L}$;

(2) tout élément a de L peut se représenter sous la forme

$a = \alpha_0 + \alpha_1 u + \ldots + \alpha_n u^n$, où $\alpha_0, \alpha_1, \ldots, \alpha_n \in K$.

La notation $\mathcal{L} = \mathcal{K}[u]$ signifie que l'anneau $\mathcal{L}$ est une extension simple de l'anneau $\mathcal{K}$ par adjonction de l'élément u. Dans ce cas l'ensemble de base de l'anneau $\mathcal{L}$ est également noté $K[u]$, $L = K[u]$.

DÉFINITION. Un anneau $\mathcal{L} = \mathcal{K}[u]$ est appelé *extension transcendante simple de l'anneau* $\mathcal{K}$ si est satisfaite la condition suivante:

(3) pour tous éléments $\alpha_0, \alpha_1, \ldots, \alpha_n$ de l'ensemble K de l'égalité $\alpha_0 + \alpha_1 u + \ldots + \alpha_n u^n = 0$ s'ensuivent les égalités $\alpha_0 = 0$, $\alpha_1 = 0, \ldots, \alpha_n = 0$.

Si $\mathcal{L} = \mathcal{K}[u]$ est une extension simple de l'anneau $\mathcal{K}$ par adjonction de u et u satisfait aux conditions (3), l'élément u est alors appelé *transcendant par rapport à* ou *sur* $\mathcal{K}$.

Si $\mathcal{K}[u]$ est une extension transcendante simple de l'anneau $\mathcal{K}$ par adjonction de u, on appelle également l'anneau $\mathcal{K}[u]$ *anneau des polynômes en u sur* $\mathcal{K}$ et les éléments de l'anneau $\mathcal{K}[u]$ *polynômes en u sur* $\mathcal{K}$ ou *polynômes sur* $\mathcal{K}$.

PROPOSITION 1.1. *Soit $\mathcal{K}[u]$ une extension transcendante simple de l'anneau $\mathcal{K}$ par adjonction de u. Alors pour tout élément a de l'anneau $\mathcal{K}[u]$, si $a = a_0 + a_1 u + \ldots + a_n u^n$ et $a = a_0' + a_1' u + \ldots + a_n' u^n$, où $a_i, a_i' \in K$, on a $a_i = a_i'$ pour $i = 1, \ldots, n$.*

D é m o n s t r a t i o n. Si

$$a = a_0 + a_1 u + \ldots + a_n u^n = a_0' + a_1' u + \ldots + a_n' u^n \quad (a_i, a_i' \in K),$$

alors

$$(1) \quad a_0 - a_0' + (a_1 - a_1')\, u + \ldots + (a_n - a_n')\, u^n = 0.$$

Par hypothèse, l'élément u est transcendant sur $\mathcal{K}$. Donc de (1) s'ensuivent les égalités $a_i - a_i' = 0$ et $a_i = a_i'$ pour $i = 0, 1, \ldots, n$. □

THÉORÈME 1.2. *Soient $\mathcal{K}$ et $\mathcal{L}$ des anneaux commutatifs, φ un isomorphisme de $\mathcal{K}$ sur $\mathcal{L}$, tandis que $\mathcal{K}[x]$ et $\mathcal{L}[y]$ sont des extensions transcendantes simples des anneaux $\mathcal{K}$ et $\mathcal{L}$ respectivement. Alors $\mathcal{K}[x] \cong \mathcal{L}[y]$ et il n'y a qu'un seul isomorphisme de l'anneau $\mathcal{K}[x]$ sur l'anneau $\mathcal{L}[y]$ faisant passer x en y et prolongeant l'isomorphisme φ de l'anneau $\mathcal{K}$ sur $\mathcal{L}$.*

Démonstration. Désignons par ψ l'application de l'anneau $\mathcal{K}[x]$ dans l'anneau $\mathcal{L}[y]$ définie de la façon suivante: pour tout $a = a_0 + \ldots + a_m x^m$ de $K[x]$ on a:

$$\psi(a_0 + \ldots + a_m x^m) = \varphi(a_0) + \ldots + \varphi(a_m) y^m.$$

On voit sans peine que ψ satisfait aux conditions: $\psi(a_0) = \varphi(a_0)$ pour tout a_0 de K, $\psi(x) = y$ et $\operatorname{Im} \psi = L[y]$.

En outre, ψ respecte les opérations principales de l'anneau $\mathcal{K}[x]$. En effet, si $a = a_0 + \ldots + a_m x^m$ et $b = b_0 + \ldots + b_n x^n$ $(m \leqslant n)$, $a, b \in K[x]$, alors

$$\begin{aligned}\psi(a+b) = \psi((a_0+b_0) + \ldots + (a_m+b_m)x^m + b_{m+1}x^{m+1} + \ldots \\ \ldots + b_{n-1}x^{n-1} + b_n x^n) = \\ = \varphi(a_0+b_0) + \ldots + \varphi(a_m+b_m)y^m + \\ + \varphi(b_{m+1})y^{m+1} + \ldots + \varphi(b_{n-1})y^{n-1} + \varphi(b_n)y^n = \\ = (\varphi(a_0) + \ldots + \varphi(a_m)y^m) + (\varphi(b_0) + \ldots \\ \ldots + \varphi(b_n)y^n) = \psi(a) + \psi(b).\end{aligned}$$

De façon analogue, on peut montrer que

$$\psi(-a) = -\psi(a), \quad \psi(ab) = \psi(a)\psi(b), \quad \psi(1_{\mathcal{K}}) = 1_{\mathcal{L}}.$$

Par conséquent, ψ est un isomorphisme de $\mathcal{K}[x]$ sur $\mathcal{L}[y]$ faisant passer x en y et prolongeant l'isomorphisme φ.

Démontrons que l'isomorphisme aux propriétés susmentionnées est unique. Supposons que ψ_1 est un autre isomorphisme de l'anneau $\mathcal{K}[x]$ sur l'anneau $\mathcal{L}[y]$ tel que $\psi_1(a_0) = \varphi(a_0)$ avec tout a_0 de K et $\psi_1(x) = y$. Alors, pour tout $a = a_0 + \ldots + a_m x^m$ de $K[x]$, on a:

$$\begin{aligned}\psi_1(a) = \psi_1(a_0) + \ldots + \psi_1(a_m)\psi_1(x^m) = \varphi(a_0) + \varphi(a_1)y + \ldots \\ \ldots + \varphi(a_m)y^m = \psi(a);\end{aligned}$$

ainsi, $\psi_1 = \psi$. □

COROLLAIRE. *Soient $\mathcal{K}[x]$ et $\mathcal{K}[y]$ deux extensions transcendantes simples d'un anneau commutatif $\mathcal{K}$. Alors $\mathcal{K}[x] \cong \mathcal{K}[y]$, et il n'existe qu'un seul isomorphisme de l'anneau $\mathcal{K}[x]$ sur l'anneau $\mathcal{K}[y]$ faisant passer x en y et induisant une application identique sur K.*

Théorème d'existence de l'extension transcendante simple d'un anneau commutatif. Soit $\mathcal{K}$ un anneau commutatif intègre. La suite infinie $a = (a_0, a_1, \ldots)$ d'éléments de K, dont tous les termes a_i à l'exception de leur nombre fini sont nuls, est appelée *suite pseudo-infinie sur* $\mathcal{K}$. Pour toute suite pseudo-infinie a il existe un nombre naturel n tel que $a_i = 0$ pour tous $i \geqslant n$. L'ensemble de toutes les suites pseudo-infinies sur $\mathcal{K}$ sera noté L_1.

Introduisons sur l'ensemble L_1 la relation d'égalité en posant $(a_0, a_1, \ldots) = (b_0, b_1, \ldots)$ si et seulement si $a_i = b_i$ pour tout nombre naturel i.

La somme de deux éléments quelconques $a = (a_0, a_1, \ldots)$ et $b = (b_0, b_1, \ldots)$ est définie par l'égalité

$$a \oplus b = (a_0 + b_0, a_1 + b_1, \ldots).$$

On notera plus loin par $(a \oplus b)_i$ la i-ième composante de la somme $a + b$.

Le produit de l'élément λ de K par l'élément a de L_1 se définit par la formule $\lambda a = (\lambda a_0, \lambda a_1, \ldots)$. En particulier, on pose $\ominus a = (-1)\, a = (-a_0, -a_1, \ldots)$.

L'addition dans L_1 est commutative, associative et est munie d'un élément neutre $\overline{0} = (0, 0, \ldots)$; de plus, pour chaque a de L_1 $\ominus a$ est un élément opposé, c'est-à-dire $a \oplus (\ominus a) = \overline{0}$. Par conséquent, l'algèbre $\langle L_1, \oplus, \ominus\rangle$ est un groupe commutatif.

Le produit de deux éléments quelconques $a = (a_0, a_1, \ldots)$ et $b = (b_0, b_1, \ldots)$ de L_1 se définit par la formule

$$(a_0, a_1, \ldots) \odot (b_0, b_1, \ldots) = (c_0, c_1, \ldots),$$

où $c_k = \sum\limits_{i+j=k} a_i b_j$ pour tout nombre naturel k. Plus loin on notera par $(a \odot b)_k$ la k-ième composante du produit ab.

Ainsi, sur l'ensemble L_1 on a défini deux opérations binaires (l'addition $\oplus$ et la multiplication $\odot$) et l'opération singulaire $\ominus$ associant à chaque a de L_1 un élément opposé $\ominus a$. Partout plus loin 1 est l'unité de l'anneau $\mathcal{K}$, $1 = 1_{\mathcal{K}}$ et $\overline{1} = (1, 0, 0, \ldots)$.

LEMME 1.3. *Une algèbre* $\mathcal{L}_1 = \langle L_1, \oplus, \ominus, \odot, \overline{1}\rangle$ *est un anneau commutatif.*

Démonstration. On a établi plus haut que l'algèbre $\langle L_1, \oplus, \ominus\rangle$ était un groupe abélien. De la définition de la multiplication dans L_1 il s'ensuit directement qu'elle est commutative. La multiplication dans L_1 est associative. En effet, pour tous a, b, c de L_1

$$(a \odot (b \odot c))_i = \sum_{j+s=i} a_j (b \cdot c)_s = \sum_{j+s=i} a_j \Big(\sum_{k+l=s} b_k c_l\Big) = \sum_{j+k+l=i} a_j b_k c_l,$$

$$((a \odot b) \odot c)_i = \sum_{t+l=i} (ab)_t c_l = \sum_{t+l=i} \left(\sum_{j+k=t} a_j b_k \right) c_l =$$
$$= \sum_{j+k+l=i} a_j b_k c_l.$$

Par conséquent, $a \odot (b \odot c) = (a \odot b) \odot c$.

La multiplication dans L_1 est distributive par rapport à l'addition. En effet, pour tous a, b, c de L_1

$$((a \oplus b) \odot c)_i = \sum_{j+k=i} (a \oplus b)_j c_k = \sum_{j+k=i} (a_j c_k + b_j c_k),$$
$$(a \odot c \oplus b \odot c)_i = (a \odot c)_i \oplus (b \odot c)_i = \sum_{j+k=i} a_j c_k + \sum_{j+k=i} b_j c_k =$$
$$= \sum_{j+k=i} (a_j c_k + b_j c_k).$$

Par conséquent, $(a \oplus b) \odot c = a \odot c \oplus b \odot c$. De plus, $\overline{1}$ est un élément neutre par rapport à la multiplication dans L_1.

Bref, on a établi que l'algèbre $\mathscr{L}_1$ est un anneau commutatif. □

Posons

$$u_0 = (1, 0, 0, \ldots), \; u_1 = (0, 1, 0, 0, \ldots), \; \ldots, \; u_k =$$
$$= (\underbrace{0, \ldots, 0}_{k \text{ zéros}}, 1, 0, \ldots).$$

Un élément quelconque $a = (a_0, a_1, \ldots)$ de L_1 peut être écrit sous la forme

$$a = a_0 (1, 0, 0, \ldots) \oplus a_1 (0, 1, 0, \ldots) \oplus \ldots$$
$$\ldots \oplus a_n (0, \ldots, 0, 1, 0, \ldots) = a_0 u_0 \oplus a_1 u_1 \oplus \ldots \oplus a_n u_n,$$

c'est-à-dire

$$a = a_0 u_0 \oplus a_1 u_1 \oplus \ldots \oplus a_n u_n,$$

où n est un nombre naturel tel que $a_i = 0$ pour tout $i > n$.

Pour tout nombre naturel n le système d'éléments $u_0, u_1, \ldots \ldots, u_n$ est linéairement indépendant sur $\mathscr{K}$, c'est-à-dire que pour tous éléments $\lambda_0, \lambda_1, \ldots, \lambda_n$ de l'ensemble K de l'égalité

(1) $\lambda_0 u_0 \oplus \lambda_1 u_1 \oplus \ldots \oplus \lambda_n u_n = \overline{0}$

s'ensuivent les égalités $\lambda_0 = 0$, $\lambda_1 = 0$, $\ldots$, $\lambda_n = 0$.

En effet, de (1) s'ensuit

$$\lambda_0 u_0 + \lambda_1 u_1 + \ldots + \lambda_n u_n =$$
$$= (\lambda_0, \lambda_1, \ldots, \lambda_n, 0, 0, \ldots) = (0, 0, 0, \ldots),$$

donc $\lambda_0 = 0$, $\lambda_1 = 0$, $\ldots$, $\lambda_n = 0$.

Posons $x = u_1 = (0, 1, 0, 0, \ldots)$. De la définition de la multiplication dans L_1, on déduit que

$$x^2 = u_2, \; x^3 = u_2 \odot u_1 = u_3, \; \ldots, \; x^n = u_{n-1} \odot u_1 = u_n.$$

Par conséquent, chaque élément a de L_1 pour lequel $a_i = 0$ avec tout $i > n$ peut être figuré sous la forme

$$a = a_0u_0 \oplus a_1u_1 \oplus \ldots \oplus a_nu_n = a_0u_0 \oplus a_1x \oplus \ldots \oplus a_nx^n.$$

THÉORÈME 1.4. *Pour chaque anneau commutatif intègre $\mathscr{K} = \langle K, +, -, \cdot, 1\rangle$ il existe une extension transcendante simple.*

D é m o n s t r a t i o n. Soit L_1 un ensemble de toutes les suites pseudo-infinies sur $\mathscr{K}$. Selon le lemme 1.3, l'algèbre

$$\mathscr{L}_1 = \langle L_1, \oplus, \ominus, \odot, \bar{1}\rangle$$

est un anneau commutatif. L'ensemble

$$K_1 = \{a_0u_0 \mid a_0 \in K\}, \quad \text{où} \quad a_0u_0 = \{a_0, 0, 0, \ldots\},$$

est fermé dans l'anneau $\mathscr{L}_1$ et n'est pas vide. Par conséquent, l'algèbre

$$\mathscr{K}_1 = \langle K, \oplus, \ominus, \odot, \bar{1}\rangle$$

est un sous-anneau de l'anneau $\mathscr{L}_1$. L'application $h_1: K_1 \rightarrow K$ telle que

$$h_1(a_0u_0) = a_0 \text{ pour chaque } a_0 \text{ de } K$$

est apparemment une application injective de l'ensemble K_1 sur K. En outre, h_1 respecte les opérations principales de l'anneau $\mathscr{K}_1$, vu que pour tous a_0, b_0 de K, on a

$$h_1(a_0u_0 \oplus b_0u_0) = a_0 + b_0,$$
$$h_1(\ominus a_0u_0) = -a_0,$$
$$h_1(a_0u_0 \odot b_0u_0) = a_0 \cdot b_0,$$
$$h_1(1 \odot u_0) = 1 \quad (\text{c'est-à-dire } h_1(\bar{1}) = 1_{\mathscr{K}}).$$

Par conséquent, h_1 est un isomorphisme de l'anneau $\mathscr{K}_1$ sur $\mathscr{K}$. Ainsi, $\mathscr{L}_1$ contient un sous-anneau $\mathscr{K}_1$ isomorphe à l'anneau $\mathscr{K}$.

Il nous faut construire sur la base de l'anneau $\mathscr{L}_1$ un nouveau anneau isomorphe à $\mathscr{L}_1$ et contenant le sous-anneau $\mathscr{K}$. Pour ce faire, substituons dans l'ensemble L_1 l'élément a_0 de K à chaque élément a_0u_0 de K_1 (autrement dit, substituons l'élément $h_1(a_0u_0)$ à a_0u_0) en laissant tous les autres éléments de l'ensemble L_1 inchangés. Posons

$$L = (L_1 \setminus K_1) \cup K$$

et définissons l'application $h\colon L_1 \to L$ de la façon suivante:

$$h(a) = \begin{cases} h_1(a) & \text{si } a \in K_1; \\ a & \text{si } a \in L_1 \setminus K_1. \end{cases}$$

On voit sans peine que h est une application injective de l'ensemble L_1 sur L qui prolonge l'application h_1, c'est-à-dire $h_1 \subset h$.

Définissons sur l'ensemble L les opérations $+$, $-$, $\cdot$, 1 par les formules

$$\text{(I)} \quad \begin{aligned} &\alpha + \beta = h(h^{-1}(\alpha) \oplus h^{-1}(\beta)) \quad (\alpha, \beta \in L); \\ &-\alpha = h(\ominus h^{-1}(\alpha)); \\ &\alpha \cdot \beta = h(h^{-1}(\alpha) \odot h^{-1}(\beta)); \\ &1 = h(\bar{1}) = 1_{\mathscr{K}}. \end{aligned}$$

Considérons l'algèbre $\mathscr{L} = \langle L, +, -, \cdot, 1\rangle$. Des formules (I) s'ensuivent les formules

$$\text{(II)} \quad \begin{aligned} &h^{-1}(\alpha + \beta) = h^{-1}(\alpha) \oplus h^{-1}(\beta); \\ &h^{-1}(-\alpha) = \ominus h^{-1}(\alpha); \\ &h^{-1}(\alpha \cdot \beta) = h^{-1}(\alpha) \odot h^{-1}(\beta); \\ &h^{-1}(1) = \bar{1}. \end{aligned}$$

Les formules (II) montrent que h^{-1} est un isomorphisme de l'algèbre $\mathscr{L}$ sur l'anneau $\mathscr{L}_1$. Il s'ensuit que l'algèbre $\mathscr{L}$ est un anneau commutatif isomorphe à l'anneau $\mathscr{L}_1$. Les opérations principales dans l'anneau $\mathscr{L}$ constituent des prolongements d'opérations correspondantes dans l'anneau $\mathscr{K}$. En effet, en vertu de (I), pour tous α et β de K, on a:

$$\begin{aligned} \alpha + \beta &= h(h^{-1}(\alpha) \oplus h^{-1}(\beta)) = h(\alpha u_0 \oplus \beta u_0) = \\ &= h(\alpha u_0) + h(\beta u_0) = h_1(\alpha u_0) + h_1(\beta u_0) = \alpha + \beta; \\ -\alpha &= h(\ominus h^{-1}(\alpha)) = h(\ominus \alpha u_0) = -h(\alpha u_0) = \\ &= -h_1(\alpha u_0) = -\alpha; \\ \alpha \cdot \beta &= h(h^{-1}(\alpha) \odot h^{-1}(\beta)) = h(\alpha u_0 \odot \beta u_0) = \\ &= h(\alpha u_0) \cdot h(\beta u_0) = h_1(\alpha u_0) \cdot h_1(\beta u_0) = \alpha\beta. \end{aligned}$$

Par conséquent, $\mathscr{K}$ est un sous-anneau de l'anneau $\mathscr{L}$.

Tout élément de $\mathscr{L}$ peut être figuré sous forme d'une combinaison linéaire d'éléments $1, x, x^2, \ldots$ avec coefficients dans K, vu que

$$\begin{aligned} h(a_0 u_0 \oplus \ldots \oplus a_n u_n) &= a_0 + a_1 u_1 + \ldots + a_n u_n = \\ &= a_0 + a_1 x + \ldots + a_n x^n \quad (a_i \in K). \end{aligned}$$

Par conséquent, $\mathscr{L} = \mathscr{K}[x]$.

L'élément x est transcendant sur $\mathscr{K}$. De fait, l'égalité

$$a_0 + a_1x + \ldots + a_nx^n = 0$$

entraîne l'égalité

$$h^{-1}(a_0 + a_1x + \ldots + a_nx^n) = a_0u_0 \oplus a_1u_1 \oplus \ldots \oplus a_nu_n = \overline{0}.$$

Puisque les éléments $u_0, \ldots, u_n$ sont linéairement indépendants sur $\mathscr{K}_1$, il s'ensuit que $a_0 = 0, a_1 = 0, \ldots, a_n = 0$. x est donc un élément transcendant sur $\mathscr{K}$ et l'anneau $\mathscr{L} = \mathscr{K}[x]$ est une extension transcendante de l'anneau $\mathscr{K}$ par adjonction de x. □

Degré d'un polynôme. Soient $\mathscr{K}$ un anneau commutatif intègre et $\mathscr{K}[x]$ un anneau des polynômes en x, c'est-à-dire une extension transcendante simple de $\mathscr{K}$ par adjonction de x. Tout élément non nul a de $K[x]$ peut être figuré de façon unique sous forme d'une combinaison linéaire de puissances de x avec coefficients dans K.

DEFINITION. Soit a un polynôme de $K[x]$. On appelle *degré du polynôme* a le nombre naturel n si $a = a_0 + a_1x + \ldots + a_nx^n$ avec $a_n \neq 0$. Dans ce cas $a_0, a_1, \ldots, a_n$ sont les *coefficients du polynôme*, l'élément a_n étant le *coefficient dominant*. Le polynôme a est dit *normé* si son coefficient dominant est égal à l'unité de l'anneau $\mathscr{K}$.

On notera le degré du polynôme a deg a.

Ainsi, le degré du polynôme se définit pour tout polynôme sauf pour le polynôme nul; le degré d'un polynôme nul ne se détermine pas. Le degré du polynôme a_0, où a_0 est un élément non nul de l'anneau $\mathscr{K}$, vaut zéro.

Notons quelques propriétés du degré d'un polynôme.

PROPOSITION 1.5. *Le degré d'une somme de deux polynômes non nuls est au plus égal au degré maximal de leurs termes, c'est-à-dire* $\deg(a + b) \leqslant \max(\deg a, \deg b)$.

PROPOSITION 1.6. *Le degré d'un produit de deux polynômes non nuls est au plus égal à la somme des degrés des cofacteurs, c'est-à-dire avec* $ab \neq 0$ $\deg(ab) \leqslant \deg a + \deg b$.

La démonstration des propositions 1.5 et 1.6 est laissée au soin du lecteur.

PROPOSITION 1.7. *Si* $\mathscr{K}$ *est un domaine d'intégrité, le degré du produit de deux polynômes non nuls est égal à la somme des degrés des cofacteurs, c'est-à-dire* $\deg(ab) = \deg a + \deg b$.

Démonstration. Soient $a = a_0 + \ldots + a_mx^m$, $b = b_0 + \ldots + b_nx^n$ des polynômes sur le domaine d'intégrité $\mathscr{K}$ et $a_m \neq 0$, $b_n \neq 0$. On a alors $ab = a_0b_0 + (a_0b_1 + a_1b_0)x + \ldots + a_mb_nx^{m+n}$. $\mathscr{K}$ étant le domaine d'intégrité, on a $a_mb_n \neq 0$. Donc, $\deg(ab) = m + n = \deg a + \deg b$. □

THEOREME 1.8. *Si* $\mathscr{K}$ *est un domaine d'intégrité, alors l'anneau des polynômes* $\mathscr{K}[x]$ *est aussi un domaine d'intégrité.*

Ce théorème découle directement de la proposition 1.7.

Des théorèmes 1.8 et 13.2.1. s'ensuit le corollaire suivant.

COROLLAIRE 1.9. *Pour un anneau des polynômes $\mathcal{K}$ $[x]$ sur le domaine d'intégrité $\mathcal{K}$ il existe un corps des quotients.*

Division d'un polynôme par un binôme et racines d'un polynôme. Soit $\mathcal{K}$ $[x]$ un anneau des polynômes en x sur un anneau commutatif intègre $\mathcal{K}$. Si $f = a_0 + a_1x + \ldots + a_nx^n \in K [x]$ et $c_0 \in K$, alors la somme $a_0 + a_1c_0 + \ldots + a_nc_0^n$ sera notée $f(c_0)$ et appelée *valeur du polynôme pour l'argument* c_0.

THÉORÈME 1.10 (de Bézout). *Soient f un polynôme sur l'anneau $\mathcal{K}$ et $c_0 \in K$. Il existe dans l'anneau $\mathcal{K}$ $[x]$ un polynôme q tel que $f =$ $= (x - c_0) q + f(c_0)$.*

Démonstration. Le théorème est vrai si f est un polynôme nul; dans ce cas $f(c_0) = 0$ et l'on peut poser $q = 0$. Soit $f = a_0 + a_1x^1 + \ldots + a_nx^n$ un polynôme non nul, alors il vient

$$f - f(c_0) = a_1 (x - c_0) + a_2 (x^2 - c_0^2) + \ldots + a_n (x^n - c_0^n) =$$
$$= (x - c_0) [a_1 + a_2 (x + c_0) + \ldots + a_n (x^{n-1} + c_0x^{n-2} + \ldots$$
$$\ldots + c_0^{n-1})];$$

par conséquent, $f = (x - c_0) q + f(c_0)$, où

$$q = a_1 + a_2 (x + c_0) + \ldots + a_n (x^{n-1} + \ldots + c_0^{n-1}) \in$$
$$\in K [x]. \square$$

Le théorème de Bézout est souvent énoncé de la façon suivante: *le reste de la division du polynôme f de $K [x]$, où $\mathcal{K}$ est un anneau commutatif, par le binôme $(x - c_0)$, $c_0 \in K$, vaut $f(c_0)$.*

Soit f un polynôme sur l'anneau $\mathcal{K}$, $c_0 \in K$.

DÉFINITION. L'élément c_0 de l'anneau $\mathcal{K}$ est appelé *racine du polynôme f sur l'anneau $\mathcal{K}$* si $f(c_0) = 0$.

THÉORÈME 1.11. *Soient f un polynôme sur l'anneau $\mathcal{K}$ et $c_0 \in K$. L'élément c_0 est une racine du polynôme f si et seulement si $x - c_0$ divise le polynôme f dans l'anneau $\mathcal{K}$* $[x]$.

Démonstration. Soit c_0 une racine du polynôme f, $f(c_0) = 0$. Selon le théorème de Bézout, $f = (x - c_0) q$, où $q \in$ $\in K [x]$. Par conséquent, $x - c_0$ divise le polynôme f dans $\mathcal{K}$ $[x]$.

Supposons maintenant que $x - c_0$ divise le polynôme f dans $\mathcal{K}$ $[x]$, c'est-à-dire $f = (x - c_0) g$, où $g \in K [x]$. Alors, $f(c_0) =$ $= (c_0 - c_0) g(c_0) = 0$. $\square$

Théorème concernant le plus grand nombre possible de racines d'un polynôme dans un domaine d'intégrité. Soit $\mathcal{K}$ $[x]$ un anneau des polynômes sur l'anneau $\mathcal{K}$.

THÉORÈME 1.12. *Soit $\mathcal{K}$ un domaine d'intégrité. Tout polynôme de $K [x]$ de degré n possède dans $\mathcal{K}$ n racines différentes au plus.*

La démonstration est menée par récurrence sur n. Si $\deg f = 0$, c'est-à-dire si $f = a_0$, où $a_0 \in K$ et $a_0 \neq 0$, alors le polynôme f n'a pas de racines. Supposons qu'un polynôme quel-

conque de $K[x]$ de degré n possède n racines au plus. Soient $f \in$ $\in K[x]$ et $\deg f = n + 1$. Si f n'a pas de racines dans $\mathscr{K}$, le théorème est alors vrai. Si, par contre, f a des racines dans $\mathscr{K}$, alors $f(c_0) = 0$ pour un certain élément c_0 de K. Selon le théorème de Bézout, $f =$ $= (x - c_0) g$, où $g \in K[x]$; de plus, puisque $\mathscr{K}$ est un domaine d'intégrité, en vertu de la proposition 1.7, le degré du polynôme g vaut n. L'élément b_0 de l'anneau $\mathscr{K}$, autre que c_0, est une racine du polynôme f si et seulement si $f(b_0) = (b_0 - c_0) g(b_0) = 0$, c'est-à-dire si $g(b_0) = 0$, vu que $\mathscr{K}$ est un domaine d'intégrité. Le degré de g étant n, par hypothèse de récurrence, g a n racines différentes au plus dans $\mathscr{K}$. Donc, le polynôme f de degré $n + 1$ possède dans $\mathscr{K}$ $n + 1$ racines différentes au plus. □

COROLLAIRE 1.13. *Si le polynôme* $f = a_0 + \ldots + a_n x^n \in$ $\in K[x]$ *possède dans le domaine d'intégrité* $\mathscr{K}$ *n racines différentes au moins, alors f est un polynôme nul.*

Egalités algébrique et fonctionnelle des polynômes. Soient $\mathscr{K}[x]$ un anneau des polynômes sur un domaine d'intégrité $\mathscr{K}$ et $f =$ $= a_0 + a_1 x + \ldots + a_n x^n \in K[x]$. Notons f^* la fonction

$$\{\langle \lambda,\ a_0 + a_1\lambda + \ldots + a_n\lambda^n \rangle \mid \lambda \in K\}$$

associant à chaque λ de K l'élément $f(\lambda) = a_0 + a_1\lambda + \ldots + a_n\lambda^n$, c'est-à-dire la valeur du polynôme f pour l'argument λ. Pour certains anneaux $\mathscr{K}$ des polynômes différents peuvent définir la même fonction. C'est ainsi par exemple, si $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}_2[x]$ est un anneau des polynômes sur le corps $\mathbb{Z}_2$, les polynômes $x + x^2$, $x - x^2$ et 0 définissent alors la même fonction.

THÉORÈME 1.14. *Soit* $\mathscr{K}[x]$ *un anneau des polynômes sur un domaine d'intégrité infini* $\mathscr{K}$. *Les polynômes f et g de* $K[x]$ *sont égaux si et seulement si sont égales les fonctions* f^* *et* g^* *qu'ils définissent.*

D é m o n s t r a t i o n. Soient f et g des polynômes de $K[x]$ et f^*, g^* les fonctions qu'ils définissent. Supposons que $f = g$. Si f et g sont des polynômes nuls, alors $f^* = g^*$. Admettons que f et g sont des polynômes non nuls de degré n:

$$f = a_0 + a_1 x + \ldots + a_n x^n, \quad g(x) = b_0 + b_1 x + \ldots + b_n x^n.$$

Comme $f = g$, on a

$$(1) \quad a_0 = b_0, \ \ldots, \ a_n = b_n.$$

Pour tout λ de K, il vient:

$$f^*(\lambda) = a_0 + a_1\lambda + \ldots + a_n\lambda^n, \quad g^*(\lambda) = b_0 + b_1\lambda + \ldots$$
$$\ldots + b_n\lambda^n.$$

Donc, en vertu, de (1), $f^* = g^*$.

Posons maintenant que $f^* = g^*$, c'est-à-dire que pour tout λ de K, on a

$$f(\lambda) = a_0 + a_1\lambda + \ldots + a_n\lambda^n = g(\lambda) = b_0 + b_1\lambda + \ldots + b_n\lambda^n.$$

Dans ce cas, pour tout polynôme $h = f - g$, est satisfaite la condition

(2) $h(\lambda) = 0$ pour tout λ de K.

L'ensemble K étant infini, (2) signifie que le polynôme h possède une infinité de racines différentes. Selon le corollaire 1.13, h est un polynôme nul, c'est-à-dire $f - g = 0$ et $f = g$. Ainsi, il s'ensuit de $f^* = g^*$ que $f = g$. □

Exercices

1. Démontrer les propositions 1.5 et 1.6.
2. Soient $\mathscr{F}[x]$ un anneau des polynômes sur le corps $\mathscr{F}$ et I un ensemble non vide de $F[x]$ fermé par rapport à la soustraction et satisfaisant aux conditions: si $f \in I$, alors $x \cdot f \in I$ et $\lambda f \in I$ pour tout λ de F. Démontrer que l'ensemble I est un idéal de l'anneau $\mathscr{F}[x]$.
3. Chercher tous les automorphismes de l'anneau des polynômes $\mathscr{Z}[x]$.
4. Chercher tous les automorphismes de l'anneau des polynômes $\mathscr{Q}[x]$.
5. Chercher tous les automorphismes de l'anneau des polynômes $\mathscr{R}[x]$.
6. Chercher tous les automorphismes de l'anneau des polynômes $\mathscr{C}[x]$ sur le corps $\mathscr{C}$ des nombres complexes.
7. Soit $\mathscr{Z}[x]$ un anneau des polynômes sur l'anneau $\mathscr{Z}$ des entiers. Montrer que l'ensemble de tous les polynômes de $Z[x]$ à termes libres pairs est un idéal de l'anneau $\mathscr{Z}[x]$ tout en n'étant pas un idéal principal.

§ 2. Polynômes sur un corps

Théorème de la division avec reste. Soient $\mathscr{F}[x]$ un anneau des polynômes sur le corps $\mathscr{F}$ et $F[x]$ son ensemble de base.

THÉORÈME 2.1. *Soit h un polynôme non nul de $F[x]$. Pour chaque polynôme f de $F[x]$ il existe dans $F[x]$ un couple unique de polynômes q et r tels que*

(1) $f = h \cdot q + r$ et $\deg r < \deg h$ ou $r = 0$.

D é m o n s t r a t i o n. Commençons par démontier par récurrence sur le degré n du polynôme f qu'il existe des polynômes q et r satisfaisant aux conditions (1). Soient

$$\deg h = m, \qquad h = b_0 + \ldots + b_m x^m \quad (b_m \neq 0).$$

Notons que si f est un polynôme nul ou $\deg f < m$, alors $f = h \cdot 0 + f$ et, par suite, on peut poser $q = 0$ et $r = f$. Il nous reste donc à étudier le cas où $\deg f \geqslant m$. Supposons que le théorème est vérifié pour tout polynôme f de degré inférieur à n. Soit $\deg f =$

$= n \geqslant m$. Dans ce cas les polynômes f et $a_n b_m^{-1} x^{n-m} h$ possèdent les mêmes coefficients dominants. Par conséquent, le polynôme

(2) $g = f - a_n b_m^{-1} x^{n-m} \cdot h$

est soit un polynôme de degré zéro, soit son degré est inférieur à n. Si $g = 0$, alors $f = a_n b_m^{-1} x^{n-m} h + 0$ et l'on peut poser $q = a_n b_m^{-1} x^{n-m}$ et $r = 0$. Si, par contre, $\deg g < n$, alors, par hypothèse de récurrence, il existe dans $F[x]$ des polynômes $\bar{q}$ et r tels que

(3) $g = h\bar{q} + r$ et $\deg r < \deg h$ ou $r = 0$.

En vertu de (2) et (3), $f = h(\bar{q} + a_n b_m^{-1} x^{n-m}) + r$ ou si l'on pose $q = \bar{q} + a_n b_m^{-1} x^{n-m}$,

(4) $f = h \cdot q + r$ et $r = 0$ ou $\deg r < \deg h$.

Démontrons que pour des polynômes f et h donnés le « quotient incomplet » q et le « reste » r dans (4) se définissent de façon univoque. En effet, supposons que

(5) $f = hq_1 + r_1$ et $r_1 = 0$ ou $\deg r_1 < \deg h$ $(r_1, q_1 \in F[x])$.

Alors, en vertu de (4) et (5), il vient

(6) $r_1 - r = h(q - q_1)$, $r_1 - r = 0$ ou $\deg (r_1 - r) < \deg h$.

Si $r_1 - r \neq 0$, alors $q - q_1 \neq 0$ et

$$\deg (r_1 - r) = \deg h + \deg (q - q_1) \geqslant \deg h,$$

ce qui est en contradiction avec les conditions (6). Mais si $r_1 - r = 0$, alors $q - q_1 = 0$ et, par suite, $q = q_1$. □

Corollaire 2.2. *Si $\mathscr{F}$ est un corps, l'anneau des polynômes $\mathscr{F}[x]$ est alors un anneau euclidien.*

Corollaire 2.3. *Un anneau des polynômes $\mathscr{F}[x]$ sur le corps $\mathscr{F}$ est un anneau des idéaux principaux.*

Corollaire 2.4. *Si $\mathscr{F}$ est un corps, l'anneau des polynômes $\mathscr{F}[x]$ est alors un anneau factoriel.*

Algorithme d'Euclide. Soit $\mathscr{K}$ un anneau commutatif.

Lemme 2.5. *Supposons qu'on ait dans un anneau commutatif $\mathscr{K}$ pour les éléments a, b, q et r l'égalité*

(1) $a = bq + r$;

alors

(2) PGCD $(a, b) \sim$ PGCD (b, r).

Démonstration. Soient $d =$ PGCD (a, b), $d' =$ PGCD (b, r). Vu que $d \mid a$, $d \mid b$, alors, en raison de (1), $d \mid r$. d étant le diviseur commun de b et r, on a $d \mid d'$. De façon analogue, on se convainc que $d' \mid d$. Par conséquent, $d \sim d'$. □

Pour trouver PGCD de deux éléments de l'anneau des polynômes $\mathcal{F}[x]$ (ou de tout anneau euclidien) on utilise le procédé « de divisions successives » appelé *algorithme d'Euclide*. Ce procédé consiste à calculer PGCD des polynômes donnés a, b de $F[x]$ en recherchant PGCD des polynômes b et r aux degrés inférieurs.

Supposons qu'aucun des polynômes a, b ne se divise (dans $\mathcal{F}[x]$) par l'autre et posons $b = b_1$; alors

$$a = b_1q_1 + b_2; \qquad \deg b_1 > \deg b_2,$$
$$b_1 = b_2q_2 + b_3, \qquad \deg b_2 > \deg b_3.$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$

Cette opération continue jusqu'à ce qu'on n'obtienne après division un reste nul:

$$b_{k-2} = b_{k-1}q_{k-1} + b_k, \qquad \deg b_{k-1} > \deg b_k,$$
$$b_{k-1} = b_kq_k + 0.$$

Notons que la suite $\deg b_1$, $\deg b_2$, ... est une suite décroissante des nombres naturels. C'est la raison de son arrêt après un nombre fini de pas. Supposons que $b_k \neq 0$ et $b_{k+1} = 0$; alors

$$\deg b_1 > \deg b_2 > \deg b_3 > \dots > \deg b_{k-1} > \deg b_k.$$

Sur la base du lemme 2.5, des égalités susmentionnées il s'ensuit

$$\text{PGCD}(a, b_1) \sim \text{PGCD}(b_1, b_2) \sim \dots \sim \text{PGCD}(b_{k-1}, b_k) \sim$$
$$\sim \text{PGCD}(b_k, 0) = b_k.$$

Ainsi, PGCD $(a, b) \sim b_k$ et b_k est PGCD (a, b).

On a abouti à la conclusion suivante. *Si aux polynômes a et b de l'anneau $\mathcal{F}[x]$ on applique l'algorithme d'Euclide, alors le dernier reste non nul ainsi obtenu est* PGCD *des polynômes a et b.*

COROLLAIRE 2.6. *Soient $\mathcal{F}$ un sous-corps du corps $\mathcal{P}$, $\mathcal{F}[x]$ et $\mathcal{P}[x]$ des anneaux des polynômes respectivement sur $\mathcal{F}$ et sur $\mathcal{P}$. Soient a et b des polynômes non simultanément nuls de $\mathcal{F}[x]$. Si d et d' sont des plus grands communs diviseurs normés des polynômes a et b respectivement dans $\mathcal{F}[x]$ et $\mathcal{P}[x]$, alors on a $d = d'$.*

Polynômes irréductibles sur un corps donné. Soit $\mathcal{F}[x]$ un anneau des polynômes sur le corps $\mathcal{F}$. Dans l'anneau $\mathcal{F}[x]$ ne sont inversibles que les polynômes de degré zéro (diviseurs unité du corps $\mathcal{F}$), c'est-à-dire les éléments non nuls du corps $\mathcal{F}$. Donc, tout polynôme de degré positif de $F[x]$ est irréversible dans l'anneau $\mathcal{F}[x]$.

Un polynôme de $F[x]$ est *réductible* ou *composé* dans l'anneau $\mathcal{F}[x]$ ou réductible sur le corps $\mathcal{F}$ si l'on peut le figurer sous forme de produit de deux polynômes de degré positif de $F[x]$.

En d'autres termes, un polynôme est réductible dans $\mathcal{F}[x]$ s'il a un degré positif et comporte des diviseurs non triviaux.

Un polynôme de $F[x]$ est *irréductible* ou *premier* dans l'anneau $\mathcal{F}[x]$ ou irréductible sur le corps $\mathcal{F}$ s'il a un degré positif et ne possède que des diviseurs triviaux, c'est-à-dire que tout diviseur du polynôme est associé soit à ce dernier, soit à l'unité.

Aussi, le polynôme a est irréductible dans l'anneau $\mathcal{F}[x]$ s'il est de degré positif e. dans toute décomposition de la forme $a = bc$, où b, $c \in F[x]$, l'un des facteurs (b ou c) est associé à l'unité du corps, et l'autre à a.

Exemples. 1. Si $\mathcal{F}$ est un corps, alors dans l'anneau des polynômes $\mathcal{F}[x]$ tout polynôme du premier degré est irréductible.

2. Dans un anneau des polynômes $\mathcal{R}[x]$, où $\mathcal{R}$ est un corps des nombres réels, le polynôme de second degré est irréductible si et seulement s'il n'admet pas de racines réelles.

PROPOSITION 2.7. *Soient p un polynôme irréductible et a tout polynôme de l'anneau $\mathcal{F}[x]$. Alors, soit p divise a, soit p et a sont premiers entre eux.*

Démonstration. On pose que $\mathcal{F}$ est un corps. Selon le corollaire 2.3, $\mathcal{F}[x]$ est un anneau d'idéaux principaux. Donc, en vertu de 13.3.9, si p ne divise pas a, on a alors $(p, a) = (1)$. Aussi a-t-on $\lambda_1 p + \lambda_2 a = 1$ pour certains λ_1, λ_2 de F. Par conséquent, selon le théorème 13.4.4, le plus grand commun diviseur de p et a vaut 1, c'est-à-dire les polynômes p et a sont premiers entre eux. □

PROPOSITION 2.8. *Soient p un polynôme irréductible dans l'anneau $\mathcal{F}[x]$ et $a_1, \ldots, a_n \in F[x]$. Si p divise le produit $a_1 a_2 \ldots a_n$, p divise alors un au moins des polynômes $a_1, a_2, \ldots, a_n$.*

Cette proposition découle directement du corollaire 2.3 et de la proposition 13.3.11.

THÉORÈME 2.9. *Soit $\mathcal{R}[x]$ un anneau des polynômes sur le corps $\mathcal{R}$ des nombres réels. L'anneau quotient $\mathcal{R}[x]/(x^2+1)$ est isomorphe au corps des nombres complexes.*

Démonstration. Soit $\mathbf{C}$ l'ensemble de base du corps $\mathscr{C}$ des nombres complexes. Soit h l'application de l'ensemble $\mathbf{R}[x]$ dans $\mathbf{C}$ telle que

$$h(f) = f(i) \text{ pour tout } f \text{ de } \mathbf{R}[x].$$

Une vérification directe montre que h est un épimorphisme de l'anneau $\mathcal{R}[x]$ sur le corps $\mathscr{C}$ des nombres complexes de noyau (x^2+1), c'est-à-dire $\operatorname{Ker} h = (x^2+1)$. Donc, selon le théorème 13.1.6 sur les épimorphismes d'anneaux, il vient $\mathcal{R}[x]/(x^2+1) \cong \mathscr{C}$. □

THÉORÈME 2.10. *Soient $\mathcal{F}[x]$ un anneau des polynômes sur le corps $\mathcal{F}$ et p un polynôme irréductible dans $\mathcal{F}[x]$. Alors l'anneau quotient $\mathcal{F}[x]/(p)$ est un corps.*

La démonstration de ce théorème est laissée au soin du lecteur.

Décomposition d'un polynôme en produit de facteurs normés

irréductibles (premiers). Soit $\mathcal{F}$ un corps, tandis que $\mathcal{F}[x]$ est un anneau des polynômes sur $\mathcal{F}$.

THÉORÈME 2.11. *Tout polynôme de degré positif de $F[x]$ peut être figuré de façon unique sous forme de produit d'un élément du corps $\mathcal{F}$ et de polynômes normés irréductibles dans $\mathcal{F}[x]$.*

Démonstration. Soit a un polynôme de degré positif de $F[x]$. L'anneau $\mathcal{F}[x]$ étant factoriel, le polynôme a peut se représenter sous forme de produit $a = q_1 \ldots q_s$ de polynômes $q_1, \ldots, q_s$ irréductibles dans l'anneau $\mathcal{F}[x]$. Soit u_k le coefficient dominant du polynôme q_k, $u_k \in F$. Alors, $q_k = u_k p_k$, où p_k est un polynôme normé irréductible dans $\mathcal{F}[x]$. Donc,

(1) $a = up_1 \ldots p_s$, où $u = u_1 \ldots u_s \in F$.

Démontrons l'unicité de la décomposition. Soit

(2) $a = vp_1^* \ldots p_s^*, \qquad v \in F,$

une décomposition quelconque dans laquelle $p_1^*, \ldots, p_s^*$ sont des polynômes normés irréductibles dans l'anneau $\mathcal{F}[x]$. L'anneau $\mathcal{F}[x]$ étant factoriel, on a: 1) $u = v$, puisque u, v sont des coefficients dominants d'un même polynôme a; 2) avec une numération adéquate les polynômes p_i et p_i^* sont associés. Vu que p_i, p_i^* sont des polynômes normés, du fait qu'ils sont associés, il découle que $p_i = p_i^*$ pour $i = 1, \ldots, s$. □

Soient $a \in F[x]$ et

(1) $a = up_1 \ldots p_s$, où $u \in F$,

est une décomposition du polynôme a en un produit de facteurs normés irréductibles dans $\mathcal{F}[x]$. Soient $p_1, \ldots, p_k$ les divers facteurs normés irréductibles du polynôme a et $\alpha_1, \ldots, \alpha_k$ les multiplicités de leur immersion dans la décomposition (1). On a alors la décomposition

(I) $a = up_1^{\alpha_1} \ldots p_k^{\alpha_k} \quad (u \in F)$.

DÉFINITION. La décomposition (I) est dite *décomposition canonique du polynôme a de $\mathcal{F}[x]$* en facteurs (normés) irréductibles sur $\mathcal{F}$.

Exercices

1. Indiquer pour quelle valeur de λ les polynômes $x^3 - 2\lambda x + \lambda^3$ et $x^3 + \lambda^2 - 2$ admettent une racine commune dans le corps des nombres complexes.

2. Chercher le plus grand commun diviseur des polynômes $x^3 - 1$ et $x^4 + x^3 + 2x^2 + x + 1$ et sa représentation linéaire en fonction de ces polynômes.

3. Chercher le plus grand commun diviseur et le plus petit commun multiple des polynômes $x^4 - 4x^3 + 1$ et $x^3 - 3x^2 + 1$.

4. Chercher le plus petit commun multiple des polynômes $x^{33} - 1$ et $x^{18} - 1$.

5. Soient $\mathcal{F}[x]$ un anneau des polynômes sur le corps $\mathcal{F}$ et a, b, c des polynômes de $F[x]$. Chercher dans $F[x]$ le plus petit idéal contenant tous ces polynômes.

6. Soit $\mathcal{F}[x]$ un anneau des polynômes sur le corps $\mathcal{F}$. Démontrer que l'ensemble de tous les multiples communs de deux polynômes donnés f et g de $F[x]$ est un idéal de l'anneau $\mathcal{F}[x]$.

7. Soient x_0 et y_0 des polynômes de $F[x]$ satisfaisant à l'égalité $ax_0 + by_0 = c$, où $a, b, c \in F[x]$. Chercher dans $F[x]$ l'ensemble de toutes les solutions de l'équation $ax + by = c$.

8. Démontrer que si le polynôme h est premier avec les polynômes f et g, h est premier avec $f \cdot g$.

9. Démontrer que le polynôme $x^4 - 2x + 3$ est irréductible sur le corps $\mathbb{Q}$.

10. Soit p un polynôme de $F[x]$ tel que tout autre polynôme de $F[x]$ est soit premier avec p, soit est divisible par p. Démontrer que le polynôme p est irréductible sur le corps $\mathcal{F}$.

11. Soit $\mathcal{F}[x]$ un anneau des polynômes sur le corps numérique $\mathcal{F}$. Soit c le degré du polynôme irréductible sur $\mathcal{F}$, $a, b \in F[x]$ et c divise ab. Démontrer que c divise a ou divise b^k pour un certain k naturel.

12. Soit $f = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$ une décomposition canonique du polynôme f sur le corps $\mathcal{F}$. Combien de diviseurs normés à coefficients dans F possède le polynôme f?

13. Soient $\mathcal{F}[x]$ un anneau des polynômes sur le corps numérique $\mathcal{F}$, p un polynôme irréductible sur $\mathcal{F}$ et I l'idéal engendré par le polynôme p. Démontrer que l'anneau quotient $\mathcal{F}[x]/I$ est un corps.

§ 3. Anneau des polynômes factoriel sur un anneau factoriel

Polynômes primitifs. Partout plus loin on utilise les notations suivantes: $\mathcal{K}$ désigne un anneau factoriel, $\mathcal{F}$ un corps des quotients de l'anneau $\mathcal{K}$; $\mathcal{K}[x]$ un anneau des polynômes en x sur $\mathcal{K}$; $\mathcal{F}[x]$ un anneau des polynômes en x sur $\mathcal{F}$.

DEFINITION. Soit $f = a_0 + a_1x + \ldots + a_nx^n$ un polynôme non nul quelconque de $K[x]$. PGCD des coefficients $a_0, a_1, \ldots, a_n$ dans l'anneau $\mathcal{K}$ est appelé *contenu du polynôme f*.

DEFINITION. Un polynôme f dont le contenu est l'unité ou le diviseur unité (dans $\mathcal{K}$) est nommé *polynôme primitif dans l'anneau* $\mathcal{K}[x]$.

Le contenu du polynôme f dans $\mathcal{K}[x]$ se définit de façon univoque aux facteurs près qui sont des diviseurs unité. En d'autres termes, deux contenus quelconques du polynôme f sont associés dans $\mathcal{K}$.

PROPOSITION. 3.1. *Si d est le contenu d'un polynôme non nul de* $K[x]$, *alors* $f = dg$, *où g est un polynôme primitif dans* $\mathcal{K}[x]$.

Démonstration. En effet, si dans le second membre de l'égalité $f = a_0 + a_1x + \ldots + a_nx^n$ on sort d des parenthèses, on obtient l'égalité $f = d\left(\frac{a_0}{d} + \frac{a_1}{d}x + \ldots + \frac{a_n}{d}x^n\right) = dg$, où, en vertu de la proposition 13.4.6, l'unité est un plus grand commun diviseur des coefficients $\frac{a_0}{d}, \frac{a_1}{d}, \ldots, \frac{a_n}{d}$ du polynôme g. Par conséquent, g est le polynôme primitif dans $\mathcal{K}[x]$. □

Notons que *tout polynôme de degré positif irréductible sur l'anneau* $\mathcal{K}$ *est primitif dans* $\mathcal{K}[x]$. En effet, si f n'est pas un polynôme primitif, alors, selon la proposition 3.1, $f = dg$, où g est le polynôme primitif dans $\mathcal{K}[x]$ de degré positif, tandis que d est le contenu de f. f étant non primitif, d n'est donc pas un diviseur unité dans $\mathcal{K}$ et, par suite, d et g sont des éléments irréversibles de $\mathcal{K}[x]$. Par conséquent, f est réductible dans $\mathcal{K}[x]$. Ainsi, tout polynôme non primitif de degré positif est réductible dans $\mathcal{K}[x]$ et, partant, tout polynôme de degré positif irréductible dans $\mathcal{K}[x]$ est un polynôme primitif dans $\mathcal{K}[x]$.

Remarquons de même qu'un polynôme primitif dans $\mathcal{K}[x]$ est réductible sur $\mathcal{K}$ si et seulement si l'on peut le représenter sous forme de produit de polynômes de degré positif (et de plus, primitifs). Pour un polynôme non primitif f quelconque cela n'est pas vrai, car il se peut que $f = dg$, où d est le contenu de f et $\deg d = 0$, tandis que g est un polynôme primitif irréductible.

LEMME 3.2. *Soient* f, h *des polynômes primitifs dans* $\mathcal{K}[x]$ *et*

(1) $cf = dh$, *où* $c, d \in K \setminus \{0\}$.

Alors d *est associé à* c *dans* $\mathcal{K}$ *et* f *est associé à* h *dans* $\mathcal{K}[x]$.

Démonstration. Soient

$$f = a_0 + \ldots + a_n x^n, \quad h = b_0 + \ldots + b_m x^m \qquad (a_n \neq 0,\ b_m \neq 0);$$

alors, $cf = ca_0 + \ldots + ca_n x^n$, $dh = db_0 + \ldots + db_m x^m$, en vertu de

(1) $n = m$ et

(2) $ca_0 = db_0, \ldots, ca_n = db_n$.

Puisque 1 est un plus grand commun diviseur des coefficients $a_0, \ldots, a_n$, en vertu de la proposition 13.4.5, c est un plus grand commun diviseur des coefficients $ca_0, \ldots, ca_n$. De façon analogue, en s'appuyant sur le fait que h est primitif et les égalités (2), on conclut que d est un plus grand commun diviseur des coefficients $ca_0, \ldots, ca_n$. Donc, c et d sont associés dans $\mathcal{K}$ et, par suite, $d = \varepsilon c$, où ε est un élément inversible de l'anneau $\mathcal{K}$. En divisant les deux membres de l'égalité (1) par c, on obtient $f = \varepsilon h$, c'est-à-dire f et h sont associés dans $\mathcal{K}[x]$. □

LEMME 3.3. *Soient* f *et* h *des polynômes primitifs dans* $\mathcal{K}[x]$. *Si les polynômes* f *et* h *sont associés dans* $\mathcal{F}[x]$, *ils sont également associés dans* $\mathcal{K}[x]$.

Démonstration. Soient f et h des polynômes associés dans $\mathcal{F}[x]$. On a alors $f = \alpha h$, où α est un élément non nul du corps $\mathcal{F}$. $\mathcal{F}$ étant un corps des quotients de l'anneau $\mathcal{K}$, l'élément α peut être représenté sous la forme $\alpha = dc^{-1}$, où $d, c \in K \setminus \{0\}$.

Ainsi, $f = dc^{-1}h$ et $cf = dh$. Selon le lemme 3.2, il s'ensuit que les polynômes f et g sont associés dans l'anneau $\mathcal{K}[x]$. □

LEMME 3.4 (DE GAUSS). *Un produit des polynômes primitifs dans $\mathcal{K}[x]$ est un polynôme primitif dans $\mathcal{K}[x]$.*

Démonstration. Soient f et g des polynômes primitifs quelconques dans $\mathcal{K}[x]$:

$$f = a_0 + a_1x + \ldots + a_mx^m \qquad (a_m \in K \setminus \{0\}),$$
$$g = b_0 + b_1x + \ldots + b_nx^n \qquad (b_n \in K \setminus \{0\});$$

dans ce cas,

$$fg = c_0 + c_1x + \ldots + c_{m+n}x^{m+n} \qquad (c_{m+n} = a_mb_n \neq 0).$$

Montrons que le polynôme fg est primitif dans l'anneau $\mathcal{K}[x]$. Supposons que p est un élément premier quelconque de l'anneau $\mathcal{K}$ et démontrons qu'un au moins des coefficients du polynôme fg ne se divise pas par p. En effet, en vertu du fait que le polynôme f est primitif, il existe un coefficient a_r non divisible par p et possédant le plus petit indice. De façon analogue, il existe un coefficient b_s du polynôme g, non divisible par p et affecté du plus petit indice. Le coefficient c_{r+s} du polynôme fg peut être représenté sous forme d'une somme:

$$(1) \quad c_{r+s} = a_rb_s + (a_{r+1}b_{s-1} + \ldots + a_{r-1}b_{s+1} + \ldots).$$

Le premier terme de cette somme n'est pas divisible par p, quant au second, il se divise par p ou manque. Ainsi, c_{r+s} ne se divise pas par p. Donc, le contenu du polynôme fg est 1, c'est-à-dire que le polynôme fg est un polynôme primitif dans $\mathcal{K}[x]$. □

LEMME 3.5. *Soit f un polynôme dans $\mathcal{K}[x]$. Si le polynôme f est réductible dans $\mathcal{F}[x]$, il est également réductible dans $\mathcal{K}[x]$.*

Démonstration. Soit un polynôme f réductible dans $\mathcal{F}[x]$, c'est-à-dire

$$(1) \quad f = gh,$$

où g et h sont des polynômes de degré positif de $F[x]$. Admettons que f est irréductible dans $\mathcal{K}[x]$ et, par suite, primitif dans $\mathcal{K}[x]$. Soit

$$g = \alpha_0 + \alpha_1x + \ldots + \alpha_nx^n.$$

Puisque $\mathcal{F}$ est un corps des quotients de l'anneau $\mathcal{K}$, chaque coefficient α_i peut être représenté sous la forme

$$\alpha_i = a_i \cdot b_i^{-1}, \text{ où } a_i, b_i \in K, \qquad (i = 0, \ldots, n).$$

Posons $b = b_0 \cdot b_1 \ldots b_n$; alors $bg \in K[x]$ et, en vertu de la proposition 3.1,

$$(2) \quad bg = cg_1 \qquad (b, c \in K \setminus \{0\}),$$

où g_1 est un polynôme de degré positif primitif dans $\mathcal{K}[x]$, tandis que c est le contenu du polynôme bg. On se convainc de façon analogue qu'il existe des éléments d et e tels que

$$(3) \quad dh = eh_1 \qquad (d, e \in K \setminus \{0\}),$$

où h_1 est un polynôme de degré positif primitif dans $\mathcal{K}[x]$.

En vertu de (1), (2) et (3), il vient

$$(4) \quad (bd) f = (ce) g_1 h_1 \qquad (bd, ce \in K \setminus \{0\}),$$

de plus, suivant le lemme de Gauss, le polynôme g_1h_1 est primitif dans $\mathcal{K}[x]$. Selon le lemme 3.2, de (4) il s'ensuit que les polynômes f et g_1h_1 sont associés dans $\mathcal{K}[x]$. Par conséquent,

$$f = \varepsilon g_1 h_1,$$

où ε est un élément inversible dans K et g_1, h_1 des polynômes de degré positif de $K[x]$, ce qui est en contradiction avec l'hypothèse admise. Ainsi, le polynôme f est réductible dans $\mathcal{K}[x]$. □

COROLLAIRE 3.6. *Si un polynôme de degré positif est irréductible dans l'anneau $\mathcal{K}[x]$, il est alors irréductible dans l'anneau $\mathcal{F}[x]$.*

Anneau factoriel des polynômes. Démontrons le principal théorème de ce paragraphe.

THÉORÈME 3.7. *Si l'anneau $\mathcal{K}$ est factoriel, l'anneau des polynômes $\mathcal{K}[x]$ l'est également.*

Démonstration. Soit $\mathcal{K}$ un anneau factoriel. Démontrons que tout élément différent de zéro et irréversible de l'anneau $\mathcal{K}[x]$ est décomposable de façon unique en un produit de facteurs premiers dans $\mathcal{K}[x]$ à l'ordre des cofacteurs et des facteurs inversibles près. Démontrons d'abord la possibilité de factorisation de cet élément. Soit f un polynôme quelconque non nul de $K[x]$. Si f est un polynôme de degré zéro, alors $f \in K$. L'anneau $\mathcal{K}$ étant factoriel, le polynôme f peut être représenté sous forme d'un produit de facteurs premiers dans $\mathcal{K}$ et, par suite, dans $\mathcal{K}[x]$. Supposons que $\deg f = n > 0$, ensuite, procédons à la décomposition en facteurs premiers de tout polynôme dont le degré est inférieur à n. Soit

$$(1) \quad f = dg(x),$$

où $d \in K$, $g(x)$ est un polynôme de degré positif primitif dans $\mathcal{K}[x]$. Si le polynôme g est irréductible sur $\mathcal{K}$, alors en décomposant dans (1) le facteur d en facteurs premiers, on obtient une factorisation de f. Mais si le polynôme $g(x)$ est réductible dans $\mathcal{K}[x]$, on peut le représenter sous forme de produit de deux polynômes de degré positif et inférieur à n: $g(x) = h(x)\varphi(x)$. Suivant l'hypothèse de récurrence $h(x)$ et $\varphi(x)$ peuvent être représentés sous forme d'un produit de facteurs premiers dans $\mathcal{K}[x]$. Par conséquent, g et, en vertu de (1), f peuvent également être représentés sous forme d'un produit de facteurs premiers.

Démontrons l'unicité de la factorisation. Soient données dans $\mathscr{K}[x]$ deux factorisations de f:

(2) $f = p_1 \ldots p_k q_1 \ldots q_s = p'_1 \ldots p'_r q'_1 \ldots q'_t,$

où p_i, $p'_i \in K$ et q_i, q'_i sont des polynômes de degré positif irréductibles et partant, primitifs. Selon les lemmes 3.2 et 3.4, il s'ensuit de (2)

(3) $p_1 \ldots p_k \sim p'_1 \ldots p'_r$ dans $\mathscr{K}$;

(4) $q_1 \ldots q_s \sim q'_1 \ldots q'_t$ dans $\mathscr{K}[x]$.

L'anneau $\mathscr{K}$ étant factoriel, on déduit de (3) que $k = r$ et pour un numérotage adéquat

(5) $p_i \sim p'_i$ dans $\mathscr{K}$, $i = 1, \ldots, k$.

Ensuite, selon le corollaire 3.6, les polynômes q_i et q'_i sont irréductibles dans l'anneau $\mathscr{F}[x]$. En vertu du fait que l'anneau $\mathscr{F}[x]$ est factoriel, il s'ensuit de (4) que $s = t$ et pour un numérotage approprié

$$q_i \sim q'_i \text{ dans } \mathscr{F}[x], \quad i = 1, \ldots, s.$$

Les polynômes q_i et q'_i sont irréductibles dans $\mathscr{K}[x]$ et, par suite, primitifs dans $\mathscr{K}[x]$, en outre, ces polynômes sont associés dans $\mathscr{F}[x]$. Par conséquent, selon le lemme 3.3, ils sont associés dans $\mathscr{K}[x]$:

(6) $q_i \sim q'_i$ dans $\mathscr{K}[x]$, $\quad i = 1, \ldots, s$.

En vertu de (5) et (6), le polynôme f présente une factorisation unique en facteurs premiers dans l'anneau $\mathscr{K}[x]$. Bref, on a montré que l'anneau $\mathscr{K}[x]$ est factoriel. □

Exercices

1. Le polynôme $x^2 + 2x + 2$ est-il réductible ou irréductible: (a) dans l'anneau $\mathscr{Q}[x]$; (b) dans l'anneau $\mathscr{R}[x]$; (c) dans l'anneau $\mathscr{C}[x]$?
2. Le polynôme $2x + 6$ est-il réductible ou irréductible: (a) dans l'anneau $\mathscr{Q}[x]$; (b) dans l'anneau $\mathscr{Z}[x]$?
3. Tout polynôme irréductible dans l'anneau $\mathscr{Z}[x]$ est un polynôme primitif dans $\mathscr{Z}[x]$. Est-ce que la réciproque est vraie?

§ 4. Dérivée formelle d'un polynôme. Facteurs multiples irréductibles

Dérivée formelle d'un polynôme. Soit $\mathscr{K}$ un anneau des polynômes en x sur le corps $\mathscr{F}$: $\mathscr{K} = \mathscr{F}[x]$. Soit $\mathscr{K}[y]$ une extension transcendante simple de l'anneau $\mathscr{K}$ par adjonction de y. L'anneau $\mathscr{K}[y]$ sera également noté $\mathscr{F}[x, y]$. Les éléments de l'anneau $\mathscr{F}[x, y]$

au cas où ils sont aussi des éléments de l'anneau $\mathcal{F}[x]$ seront notés $f(x)$, $g(x)$, etc. ; et s'ils sont des éléments de l'anneau $\mathcal{F}[y]$, on les notera $f(y)$, $g(y)$, etc.

Considérons dans l'anneau $\mathcal{F}[x, y]$ les polynômes

$$f(x) = a_0 + a_1x + \ldots + a_nx^n \quad (a_i \in F),$$
$$f(y) = a_0 + a_1y + \ldots + a_ny^n$$

ainsi que leur différence $f(x) - f(y)$. On voit sans peine que

$$f(x) - f(y) = \sum_{k=1}^{n} a_k (x^k - y^k) =$$
$$= (x-y) \sum_{k=1}^{n} a_k (x^{k-1} + x^{k-2}y + \ldots + y^{k-1}) =$$
$$= (x-y)\,\Phi(x, y),$$

où $\Phi(x, y) = \sum_{k=1}^{n} a_k (x^{k-1} + x^{k-2}y + \ldots + y^{k-1})$. Notons que

$$\Phi(x, x) = \sum_{k=1}^{n} ka_kx^{k-1} = a_1 + 2a_2x + \ldots + na_nx^{n-1}.$$

DÉFINITION. Soit $f = a_0 + a_1x + \ldots + a_nx^n$ un polynôme sur le corps $\mathcal{F}$. Le polynôme

$$\Phi(x, x) = \sum_{k=1}^{n} ka_kx^{k-1} = a_1 + 2a_2x + \ldots + na_nx^{n-1}$$

est appelé *dérivée formelle du polynôme* f (ou *polynôme dérivé*) et noté f' ou $f'(x)$.

THÉORÈME 4.1. *Soient* $\mathcal{F}[x]$ *un anneau des polynômes sur le corps* $\mathcal{F}$, f, g *des polynômes quelconques de* $F[x]$ *et* $\lambda \in F$; *on a alors*

(1) $(f + g)' = f' + g'$;

(2) $(fg)' = fg' + f'g$;

(3) $(\lambda f)' = \lambda f'$;

(4) $(f^m)' = mf^{m-1}f'$ *pour tout* m *naturel.*

Démonstration. (1) Soit $h = f + g$; alors

$$f(x) - f(y) = (x - y)\,\Phi(x \cdot y), \quad g(x) - g(y) = (x - y)\,G(x, y),$$
$$h(x) - h(y) = f(x) - f(y) + g(x) - g(y) =$$
$$= (x - y)\,[\Phi(x, y) + G(x, y)].$$

Donc, $h' = \Phi(x, x) + G(x, x) = f' + g'$; par conséquent, $(f + g)' = f' + g'$.

(2) Posons $\varphi = fg$, alors

$$\varphi(x) - \varphi(y) = f(x)g(x) - f(y)g(y) =$$
$$= f(x)(g(x) - g(y)) + g(y)(f(x) - f(y)) =$$
$$= (x - y)[f(x)G(x, y) + g(y)\Phi(x, y)].$$

De là on obtient

$$\varphi' = f(x)G(x, x) + g(x)\Phi(x, x) = f(x)g'(x) + g(x)f'(x);$$

par conséquent, $(fg)' = fg' + f'g$.

(3) La formule (3) se déduit directement de la formule (2) pour $g = \lambda$, car dans ce cas $g' = 0$.

(4) La démonstration de la formule (4) s'effectue par récurrence sur m en la formule (2). □

Décomposition d'un polynôme suivant les puissances de la différence $x - c$. Avec la division du polynôme $f = a_0x^n + \ldots$ $\ldots + a_n$ par un binôme de la forme $x - c$, il est commode de disposer les calculs suivant un schéma (appelé *schéma de Horner*):

	a_0	a_1	a_2	...	a_{n-1}	a_n
c	b_0	b_1	b_2	...	b_{n-1}	r
	a_0	$cb_0 + a_1$	$cb_1 + a_2$	...	$cb_{n-2} + a_{n-1}$	$cb_{n-1} + a_n$

Apparemment, $a_0 = b_0$; tout coefficient suivant du quotient et le reste r se calculent par les formules

$$b_k = cb_{k-1} + a_k \quad (k = 1, \ldots, n - 1); \quad r = cb_{n-1} + a_n.$$

Ces formules sont obtenues à partir de l'égalité

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n =$$
$$= (x - c)(b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}) + r,$$

après avoir supprimé les parenthèses, réduit les termes semblables et égalé l'un à l'autre les coefficients associés aux mêmes puissances dans les deux membres de l'égalité.

Le schéma de Horner est commode lorsqu'on effectue une décomposition du polynôme donné f suivant les puissances du binôme $x - c$.

Soient

$$f = (x - c)q_1 + r_0,$$
$$q_1 = (x - c)q_2 + r_1,$$

(1) $\quad \ldots\ldots\ldots\ldots\ldots$

$$q_{n-2} = (x - c)q_{n-1} + r_{n-2},$$
$$q_{n-1} = (x - c)a_0 + r_{n-1}.$$

où q_k et r_k désignent le quotient et le reste obtenus après division de q_{k-1} par $x - c$. Si la dernière expression dans (1) de q_{k-1} est portée dans l'égalité précédente, ensuite, la quantité ainsi obtenue est substituée à q_{n-2}, etc., on aboutit à l'égalité

$$(2) \quad f = r_0 + r_1 (x - c) + r_2 (x - c)^2 + \dots \\ \dots + r_{n-1} (x - c)^{n-1} + a_0 (x - c)^n.$$

C'est, précisément, la décomposition du polynôme donné f en puissances de $(x - c)$. Dérivons les deux membres de l'égalité (2) et, en posant $x = c$, il vient

$$f(c) = r_0, \quad f'(c) = r_1, \quad f''(c) = 2!\, r_2, \dots, f^{(n)}(c) = n!\, a_0.$$

Aussi peut-on écrire l'égalité (2) sous la forme

$$f = f(c) + f'(c)(x - c) + \frac{f''(c)}{2!}(x - c)^2 + \dots + \frac{f^{(n)}(c)}{n!}(x - c)^n$$

si seulement f est un polynôme sur un corps de caractéristique nulle. C'est, précisément, la *formule de Taylor* pour les polynômes. La division suivant le schéma de Horner de f par $x - c$ fournit les coefficients du quotient q_1 qu'il faut à son tour diviser par $x - c$, etc. ; il est commode de disposer tous les calculs sous forme d'un tableau :

	a_0	a_1	$\dots$	a_{n-1}	a_n	
c	b_0	b_1	$\dots$	b_{n-1}	r_0	$r_0 = f(c)$
	c_0	c_1	$\dots$	r_1		$r_1 = f'(c)$
	d_0	d_1	$\dots$			$r_2 = f''(c)$
	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
	a_0	r_{n-1}				$r_{n-1} = \frac{f^{(n-1)}(c)}{(n-1)!}$

Facteurs multiples irréductibles d'un polynôme. Soit $\mathcal{F}[x]$ un anneau des polynômes sur le corps $\mathcal{F}$ de caractéristique nulle.

DÉFINITION. Soient f un polynôme de $F[x]$ et p son facteur irréductible. On appelle *facteur de multiplicité m* (ou *facteur multiple d'ordre m*) du polynôme f le polynôme p si

$$(1) \quad f = p^m g, \qquad p \nmid g, \qquad g \in F[x].$$

Pour $m > 1$ le polynôme p est appelé *facteur multiple* et pour $m = 1$ *facteur premier du polynôme f*.

THÉORÈME 4.3. *Soient $\mathscr{F}[x]$ un anneau des polynômes sur le corps $\mathscr{F}$ de caractéristique nulle et $f \in F[x]$. Soit p un facteur irréductible de multiplicité $m \geqslant 1$ du polynôme f. p est alors un facteur de multiplicité $m - 1$ de la dérivée f'.*

Démonstration. Par hypothèse, p est un facteur multiple d'ordre m du polynôme f et, par suite, la condition (1) est satisfaite. En se servant des propriétés de la dérivée, on obtient

$$f' = mp^{m-1}p'g + p^m g',$$

$$f' = p^{m-1}(mp'g + pg'). \tag{2}$$

Vu que par hypothèse le corps $\mathscr{F}$ a une caractéristique nulle, on a $mp' \neq 0$ et $\deg(mp') < \deg p$; donc $p \nmid mp'$. p étant un polynôme irréductible et (en raison de (1)) $p \nmid g$, il s'ensuit que $p \nmid (mp')g$, donc

$$p \nmid (mp'g + pg'). \tag{3}$$

Sur la base de (2) et (3) on conclut que p est un facteur de multiplicité $m - 1$ de la dérivée f'. □

COROLLAIRE 4.4. *Le polynôme f de $F[x]$ possède des facteurs multiples irréductibles si et seulement si le plus grand commun diviseur des polynômes f et f' est de degré positif.*

Racines multiples d'un polynôme. Soient $\mathscr{F}[x]$ un anneau des polynômes sur le corps $\mathscr{F}$ et $F[x]$ son ensemble de base.

DÉFINITION. Soient f un polynôme de $F[x]$ et c sa racine dans $\mathscr{F}$. L'élément c est appelé *racine de multiplicité m* (ou *racine multiple d'ordre m*) si $f = (x - c)^m g$, $g(c) \neq 0$, $g \in F[x]$; pour $m > 1$ l'élément c est appelé *racine multiple* et pour $m = 1$ il est appelé *racine simple du polynôme f*.

PROPOSITION 4.5. *Soient $\mathscr{F}[x]$ un anneau des polynômes sur un corps de caractéristique nulle et $f \in F[x]$. L'élément c de F est une racine multiple du polynôme f si et seulement si $f(c) = f'(c) = 0$.*

Cette proposition découle directement du théorème 1.9 et du corollaire 4.4.

PROPOSITION 4.6. *Soient $\mathscr{F}[x]$ un anneau des polynômes sur le corps $\mathscr{F}$ de caractéristique nulle et $f \in F[x]$. L'élément c est une racine multiple d'ordre m du polynôme f si et seulement si*

$$f(c) = f'(c) = \ldots = f^{(m-1)}(c) = 0, \quad f^{(m)}(c) \neq 0. \tag{1}$$

Démonstration. Selon le théorème 4.3, l'élément c est une racine multiple d'ordre m du polynôme f (c'est-à-dire $(x - c)$ est un facteur multiple d'ordre m du polynôme f) si et seulement si

$$(x - c) \text{ divise } f, f', \ldots, f^{(m-1)} \text{ et } (x - c) \nmid f^{(m)}. \tag{2}$$

En vertu du théorème de Bézout les conditions (1) et (2) sont équipotentes. □

Exercices

1. Décomposer le polynôme $x^6 - 5x^5 + 3x^3 - 1$ en puissances de $x - 1$.
2. Décomposer le polynôme $x^5 + 4x^4 - x^3 - 29x^2 - 14x - 1$ en puissances de la différence $x - 2$.
3. Décomposer le polynôme $x^5 - x^3 + 1$ en puissances de $x + i$.
4. Calculer les valeurs du polynôme $x^4 + 3x^2 - 5x + 1$ et de ses dérivées pour $x = -1$.
5. Déterminer la multiplicité de la racine 1 du polynôme $x^6 - x^5 - x^4 + 2x^3 - x^2 - x + 1$.
6. Déterminer la multiplicité de la racine i du polynôme $x^6 + x^5 + 3x^4 + 2x^3 + 3x^2 + x + 1$.
7. Déterminer les coefficients a et b de manière que le polynôme $ax^4 + bx^3 + 1$ de $\mathbf{Q}[x]$ soit divisible par $(x - 1)^2$.
8. Déterminer les coefficients a et b de manière que le polynôme $ax^{n+1} + bx^n + 1$ de $\mathbf{Q}[x]$ soit divisible par $(x - 1)^2$.
9. Déterminer le coefficient a de manière que le polynôme $x^5 - ax^2 - ax + 1$ de $\mathbf{Q}[x]$ admette -1 pour racine de multiplicité non inférieure à 2.
10. Chercher à quelles conditions le polynôme $x^5 + ax^3 + b$ possède dans le corps des nombres complexes une racine double autre que zéro.
11. Le polynôme $x^n + a$, où n est un nombre naturel et a un nombre non nul, a-t-il des racines multiples dans le corps des nombres complexes?
12. Démontrer que le polynôme $1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!}$ est démuni de racines multiples dans tout corps numérique.
13. Soient $\mathscr{F}$ et $\mathscr{P}$ des corps numériques, $\mathscr{F}$ étant un sous-corps du corps $\mathscr{P}$. Démontrer que si le polynôme f est irréductible dans l'anneau des polynômes $\mathscr{F}[x]$, il est démuni de facteurs multiples dans l'anneau $\mathscr{P}[x]$.

CHAPITRE XV

POLYNÔMES À PLUSIEURS VARIABLES

§ 1. Anneau des polynômes à plusieurs variables

Extension multiple d'un anneau. Soient $\mathcal{K}$ un sous-anneau intègre de l'anneau commutatif $\mathcal{L}$ et $x_1, \ldots, x_m$ des éléments de l'anneau $\mathcal{L}$.

DÉFINITION. Une extension minimale de l'anneau $\mathcal{K}$, qui est un sous-anneau de l'anneau $\mathcal{L}$ et contient les éléments $x_1, \ldots, x_m$ de L, est appelée *sous-anneau de l'anneau* $\mathcal{L}$ engendré par l'anneau $\mathcal{K}$ et les éléments $x_1, \ldots, x_m$.

Cet anneau est noté $\mathcal{K}[x_1, \ldots, x_m]$ et son ensemble de base, $K[x_1, \ldots, x_m]$.

L'anneau $\mathcal{K}[x_1, \ldots, x_m]$ est apparemment une intersection de tous les sous-anneaux de l'anneau $\mathcal{L}$ contenant les éléments $x_1, \ldots, x_m$ et ayant l'anneau $\mathcal{K}$ en qualité de sous-anneau.

DÉFINITION. Un anneau noté $\mathcal{K}[x_1] \ldots [x_m]$ et défini par induction au moyen des formules

$$\mathcal{K}[x_1][x_2] = (\mathcal{K}[x_1])[x_2],$$

$$\mathcal{K}[x_1][x_2] \ldots [x_m] = (\mathcal{K}[x_1][x_2] \ldots [x_{m-1}])[x_m],$$

est appelé *extension multiple d'ordre m de l'anneau* $\mathcal{K}$.

THÉORÈME 1.1. *Soient* $\mathcal{K}$ *un sous-anneau de l'anneau commutatif* $\mathcal{L}$ *et* $x_1, \ldots, x_m \in L$; *alors*

(1) $$\mathcal{K}[x_1, x_2, \ldots, x_m] = \mathcal{K}[x_1][x_2] \ldots [x_m].$$

Démonstration. Le théorème est apparemment vrai pour $m = 1$. Supposons que le théorème est vrai quand on adjoint $m - 1$ éléments à l'anneau $\mathcal{K}$. Par définition, on a

$$K[x_1, \ldots, x_{m-1}] \subset K[x_1, \ldots, x_m] \text{ et } x_m \in K[x_1, \ldots, x_m],$$

aussi a-t-on

(2) $$(K[x_1, \ldots, x_{m-1}])[x_m] \subset K[x_1, \ldots, x_m].$$

D'autre part, puisque $x_1, \ldots, x_m \in (K[x_1, \ldots, x_m])[x_m]$, on a

(3) $$K[x_1, \ldots, x_m] \subset (K[x_1, \ldots, x_{m-1}])[x_m].$$

En vertu de (2) et (3), il vient

(4) $K[x_1, \ldots, x_{m-1}, x_m] = K[x_1, \ldots, x_{m-1}][x_m]$.

Par hypothèse de récurrence, on a

(5) $K[x_1, \ldots, x_{m-1}] = K[x_1] \ldots [x_{m-1}]$.

Sur la base des égalités (4) et (5), on conclut que

$$K[x_1, x_2, \ldots, x_m] = K[x_1][x_2] \ldots [x_m].$$

Par conséquent, la formule (1) est vraie. □

Anneau des polynômes à plusieurs variables. Soient m un entier positif et N un ensemble de tous les nombres naturels. Soient $\mathrm{N}^1 = \mathrm{N}$ et pour $m > 1$

$$\mathrm{N}^m = \{(i_1, \ldots, i_m) \mid i_1, \ldots, i_m \in \mathrm{N}\},$$

où $(i_1, \ldots, i_m)$ est un vecteur à m dimensions.

Selon le théorème 1.1, $\mathscr{K}[x_1, x_2] = (\mathscr{K}[x_1])[x_2]$. Aussi, les éléments de l'anneau $\mathscr{K}[x_1, x_2]$ constituent-ils une somme de la forme

$$\alpha_0 + \alpha_1 x_2 + \ldots + \alpha_n x_2^n,$$

où $\alpha_i = a_{i0} + a_{i1}x_1 + \ldots + a_{im}x_1^m$ $(a_{ik} \in K)$, et m est la puissance la plus élevée des polynômes $\alpha_0, \alpha_1, \ldots, \alpha_n$. Donc, les éléments de l'anneau $\mathscr{K}[x_1, x_2]$ peuvent être écrits sous la forme

$$\sum_{(i_1, i_2) \in M} a_{i_1 i_2} x_1^{i_1} x_2^{i_2} \qquad (a_{i_1 i_2} \in K),$$

où M est un sous-ensemble fini non vide de l'ensemble $\mathrm{N}^2 = \mathrm{N} \times \mathrm{N}$.

En se basant sur le théorème 1.1, on conclut également que les éléments de l'anneau $\mathscr{K}[x_1, \ldots, x_m]$ sont une somme de la forme

$$\sum_{(i_1, \ldots, i_m) \in M} a_{i_1 \ldots i_m} x_1^{i_1} \ldots x_m^{i_m},$$

où M est un sous-ensemble fini non vide de l'ensemble N^m et $a_{i_1 \ldots i_m} \in K$. On écrira cette somme sous forme condensée

$$\sum_{(i) \in M} a_{(i)} x_1^{i_1} \ldots x_m^{i_m}, \text{ où } (i) = (i_1, \ldots, i_m).$$

Rappelons que l'élément x_1 de l'anneau $\mathscr{K}[x_1]$ est dit *transcendant sur* $\mathscr{K}$ si pour tous éléments $a_1, \ldots, a_n$ de l'anneau $\mathscr{K}$ de l'égalité $\sum_{i=1}^{n} a_i x_1^i = 0$ s'ensuivent les égalités $a_1 = 0, \ldots, a_n = 0$. La généralisation de cette notion est la notion de l'indépendance algébrique de la collection d'éléments $x_1, \ldots, x_m$ sur $\mathscr{K}$.

Soit $\mathscr{K}$ un sous-anneau de l'anneau commutatif $\mathscr{L}$.

DÉFINITION. Les éléments $x_1, \ldots, x_m$ de l'anneau $\mathscr{L}$ sont dits *algébriquement indépendants* ou simplement *algébriques sur l'anneau*

$\mathcal{K}$ si pour tous éléments $a_{(i)}$ de l'anneau $\mathcal{K}$ de l'égalité

$$\text{(I)} \qquad \sum_{(i)\in M} a_{(i)} x_1^{i_1} \ldots x_m^{i_m} = 0, \quad \text{où } M \subset \mathbf{N}^m,$$

s'ensuit l'égalité à zéro de tous les coefficients $a_{(i)}$.

Pour $m = 1$ on aboutit à la définition de l'élément algébriquement indépendant (ou algébrique) sur $\mathcal{K}$ qui coïncide avec la définition de l'élément transcendant sur $\mathcal{K}$.

THÉORÈME 1.2. *Soient $\mathcal{K}$ un sous-anneau de l'anneau commutatif $\mathcal{L}$ et $x_1, \ldots, x_m \in L$. Les éléments $x_1, \ldots, x_m$ sont algébriques sur $\mathcal{K}$ si et seulement si pour chaque $s \in \{1, \ldots, m\}$ l'élément x_s est transcendant sur $\mathcal{K}[x_1, \ldots, x_{s-1}]$.*

Démonstration. Supposons que les éléments $x_1, \ldots, x_m$ sont algébriques sur $\mathcal{K}$ et démontrons que pour chaque $s \in \{1, \ldots, m\}$ l'élément x_s est transcendant sur l'anneau $\mathcal{K}[x_1, \ldots, x_{s-1}]$.

Soit

$$\text{(II)} \quad A_0 + A_1 x_s + \ldots + A_l x_s^l = 0, \quad \text{où} \quad A_k \in K[x_1, \ldots, x_{s-1}].$$

Les termes $A_k x_s^k$ peuvent prendre la forme

$$A_k x_s^k = \sum_{(i)\in M_k} a_{(i)} x_1^{i_1} \ldots x_{s-1}^{i_{s-1}} x_s^k x_{s+1}^0 \ldots x_m^0, \quad \text{où } M_k \subset \mathbf{N}^m,$$

$$k = 0, \ldots, l.$$

L'égalité (II) peut alors être écrite ainsi:

$$(3) \qquad \sum_{(i)\in \cup M_k} a_{(i)} x_1^{i_1} \ldots x_s^{i_s} x_{s+1}^0 \ldots x_m^0 = 0.$$

En vertu de l'indépendance algébrique des éléments $x_1, \ldots, x_m$ sur l'anneau $\mathcal{K}$ il s'ensuit de (3) l'égalité à zéro de tous les coefficients $a_{(i)}$ pour $(i) \in \bigcup M_k$, donc, $A_k = 0$ pour $k = 0, 1, \ldots, l$. Par conséquent, pour chaque $s \in \{1, \ldots, m\}$ l'élément x_s est transcendant sur $\mathcal{K}[x_1, \ldots, x_{s-1}]$.

Supposons que pour chaque $s \in \{1, \ldots, m\}$ l'élément x_s est transcendant sur $\mathcal{K}[x_1, \ldots, x_{s-1}]$ et démontrons par récurrence sur m que de (I) s'ensuit l'égalité à zéro de tous les coefficients $a_{(i)}$.

Pour $m = 1$ l'affirmation est apparemment vraie. Admettons que l'affirmation est vraie pour la collection d'éléments $x_1, \ldots, x_{m-1}$. Ecrivons l'égalité (I) sous la forme

$$(4) \quad A_0 + A_1 x_m + A_2 x_m^2 + \ldots + A_r x_m^r = 0,$$

où

$$A_k x_m^k = \sum_{(i)\in M_k} a_{(i)} x_1^{i_1} \ldots x_{m-1}^{i_{m-1}} x_m^k,$$

$$A_k \in K[x_1, \ldots, x_{m-1}], \qquad M = \bigcup_k M_k.$$

Par hypothèse, l'élément x_m est transcendant sur $\mathcal{K}[x_1, \ldots, x_{m-1}]$, donc, de (4) s'ensuivent les égalités $A_0 = 0$, $A_1 = 0, \ldots, A_r = 0$. Par hypothèse de récurrence, s'ensuivent les égalités

$$a_{(i)} = 0 \text{ pour } (i) \in \bigcup M_k = M.$$

Par conséquent, les éléments $x_1, \ldots, x_m$ sont algébriques sur $\mathcal{K}$. □

Soient $\mathcal{K}$ un anneau commutatif intègre et $\mathcal{K}[x_1] \ldots [x_m]$ une extension multiple d'ordre k de l'anneau $\mathcal{K}$ par adjonction des éléments $x_1, \ldots, x_m$. Selon le théorème 1.1, $\mathcal{K}[x_1 \ldots x_m] = \mathcal{K}[x_1] \ldots [x_m]$ et, par suite, l'anneau $\mathcal{K}[x_1, \ldots, x_m]$ est également une extension multiple d'ordre k de l'anneau $\mathcal{K}$.

Définition. L'anneau $\mathcal{K}[x_1, \ldots, x_m]$ est appelé *extension transcendante multiple d'ordre m de l'anneau* $\mathcal{K}$ si pour tout $s \in \{1, \ldots, m\}$ l'anneau $\mathcal{K}[x_1, \ldots, x_s]$ est une extension transcendante simple de l'anneau $\mathcal{K}[x_1, \ldots, x_{s-1}]$ par adjonction de x_s.

Remarquons que pour $m = 1$ l'extension transcendante multiple d'ordre m de l'anneau $\mathcal{K}$ est une extension transcendante simple de l'anneau $\mathcal{K}$.

Théorème 1.3. *Soit $\mathcal{K}$ un anneau commutatif non réduit à $\{0\}$. Pour tout m naturel différent de zéro il existe une extension transcendante multiple d'ordre m de l'anneau $\mathcal{K}$. De plus, si $\mathcal{K}$ est un domaine d'intégrité, alors l'extension transcendante multiple d'ordre m de cet anneau constitue également un domaine d'intégrité.*

Démonstration. En s'appuyant sur le théorème 14.1.2 sur l'existence d'une extension transcendante simple d'un anneau, on est en mesure de construire successivement les anneaux:

$$\mathcal{K}[x_1],$$
$$(\mathcal{K}[x_1])[x_2],$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$(\mathcal{K}[x_1] \ldots [x_{m-1}])[x_m],$$

où $\mathcal{K}[x_1]$ est une extension transcendante simple de l'anneau $\mathcal{K}$ par adjonction de x_1, $(\mathcal{K}[x_1])[x_2]$ une extension transcendante simple de l'anneau $\mathcal{K}[x_1]$ par adjonction de x_2, etc. Et enfin, $(\mathcal{K}[x_1] \ldots [x_{m-1}])[x_m]$ une extension transcendante simple de l'anneau $\mathcal{K}[x_1] \ldots [x_{m-1}]$ par adjonction de x_m. Par définition précédant le théorème, ce dernier anneau est une extension transcendante multiple d'ordre m de l'anneau $\mathcal{K}$. De plus, selon le théorème 14.1.6, si $\mathcal{K}$ est un domaine d'intégrité, tous les anneaux construits plus haut sont des domaines d'intégrité. □

Définition. L'anneau $\mathcal{K}[x_1, \ldots, x_m]$ constituant une extension transcendante multiple d'ordre m d'un anneau commutatif intègre $\mathcal{K}$ est appelé *anneau des polynômes sur $\mathcal{K}$ en $x_1, \ldots, x_m$*.

Parfois, si nécessaire, les éléments f, g, etc., de cet anneau sont également notés $f(x_1, \ldots, x_m)$, $g(x_1, \ldots, x_m)$, etc.

Isomorphisme d'anneaux des polynômes. Soient $\mathcal{K}$ et $\mathcal{L}$ des anneaux commutatifs intègres.

THÉORÈME 1.4. *Soient $\mathcal{K}$ et $\mathcal{L}$ des anneaux isomorphes et φ un isomorphisme de $\mathcal{K}$ sur $\mathcal{L}$, $\mathcal{K}[x_1, \ldots, x_n]$, $\mathcal{L}[y_1, \ldots, y_n]$ étant des anneaux des polynômes. Il existe alors un isomorphisme de l'anneau $\mathcal{K}[x_1, \ldots, x_n]$ sur l'anneau $\mathcal{L}[y_1, \ldots, y_n]$ faisant passer $x_1, \ldots, x_n$ en $y_1, \ldots, y_n$ respectivement et prolongeant l'isomorphisme φ.*

D é m o n s t r a t i o n. Effectuons la récurrence sur n. Si $n = 1$, alors, selon le théorème 14.1.2, il existe un isomorphisme φ_1 de l'anneau $\mathcal{K}[x_1]$ sur l'anneau $\mathcal{L}[y_1]$ tel que $\varphi_1(x_1) = y_1$ et $\varphi_1(a) = \varphi(a)$ pour tout élément a de K.

Admettons qu'il existe un isomorphisme φ_n de l'anneau $\mathcal{K}[x_1, \ldots, x_n]$ sur l'anneau $\mathcal{L}[y_1, \ldots, y_n]$ faisant passer $x_1, \ldots, x_n$ en $y_1, \ldots, y_n$ respectivement et prolongeant l'isomorphisme φ. Alors, selon le théorème 14.1.2, il existe un isomorphisme φ_{n+1} de l'anneau $(\mathcal{K}[x_1 \ldots x_n])[x_{n+1}]$ sur l'anneau $(\mathcal{L}[y_1, \ldots, y_n])[y_{n+1}]$ faisant passer x_{n+1} en y_{n+1} et prolongeant l'isomorphisme φ_n. Compte tenu de ce que, selon le théorème 1.1,

$$(\mathcal{K}[x_1, \ldots, x_n])[x_{n+1}] = \mathcal{K}[x_1, \ldots, x_{n+1}] \text{ et}$$
$$(\mathcal{L}[y_1, \ldots, y_n])[y_{n+1}] = \mathcal{L}[y_1, \ldots, y_{n+1}],$$

on aboutit à ce que φ_{n+1} est un isomorphisme de $\mathcal{K}[x_1, \ldots, x_{n+1}]$ sur $\mathcal{L}[y_1, \ldots, y_{n+1}]$ faisant passer les éléments $x_1, \ldots, x_{n+1}$ en $y_1, \ldots, y_{n+1}$ respectivement et prolongeant l'isomorphisme φ.

Ainsi, l'affirmation du théorème est vraie pour tout nombre naturel n. □

COROLLAIRE 1.5. *Soient $\mathcal{K}[x_1, \ldots, x_n]$ et $\mathcal{K}[y_1, \ldots, y_n]$ des anneaux des polynômes sur l'anneau $\mathcal{K}$. Il existe alors un isomorphisme φ de l'anneau $\mathcal{K}[x_1, \ldots, x_n]$ sur l'anneau $\mathcal{K}[y_1, \ldots, y_n]$ faisant passer $x_1, \ldots, x_n$ en $y_1, \ldots, y_n$ respectivement et tel que $\varphi(a) = a$ pour tout élément de l'anneau $\mathcal{K}$.*

Représentation normale d'un polynôme et degré d'un polynôme. Soient N un ensemble de tous les nombres naturels et m un nombre naturel fixé différent de zéro. Pour tout nombre naturel k définissons l'ensemble S_k:

$$S_k = \{(i_1, \ldots, i_m) \in \mathrm{N}^k \mid i_1 + \ldots + i_m = k\}.$$

Notons que

(1) $\quad S_l \cap S_k = \varnothing$ pour $l \neq k$.

Le polynôme $\sum\limits_{(i) \in M} a_{(i)} x_1^{i_1} \ldots x_m^{i_m}$ est dit *nul* si tous les coefficients $a_{(i)}$ sont nuls.

THÉORÈME 1.6. *Soit f un polynôme non nul de l'anneau des polynômes $\mathcal{K}[x_1, \ldots, x_m]$. Il existe pour le polynôme f un nombre natu-*

rel n et une représentation telle que

$$(2)\quad f=\sum_{k=0}^{n}\Big(\sum_{(i)\in S_k} a_{(i)}x_1^{i_1}\dots x_m^{i_m}\Big),\ \text{où}\ a_{(i)}\in K,$$

pour laquelle au moins un coefficient $a_{(i)}$ non nul vérifie la relation $i_1+\ldots+i_m=n$. Cette représentation est unique en ce sens que si

$$(3)\quad f=\sum_{k=0}\Big(\sum_{(i)\in S_k} b_{(i)}x_1^{i_1}\dots x_m^{i_m}\Big),\ \text{où}\ b_{(i)}\in K,$$

est une autre représentation, on a alors $s=n$ et $a_{(i)}=b_{(i)}$ pour tous les (i) de S_k avec $k=0, 1, \ldots, n$.

Démonstration. Soit

$$(4)\quad f=\sum_{(i)\in M} a_{(i)}x_1^{i_1}\dots x_m^{i_m}\quad (a_{(i)}\in K),$$

où M est un sous-ensemble fini do l'ensemble $\mathbf{N}^m$. Il n'y a pas dans cette somme de termes semblables et, puisque f est un polynôme non nul, il existe dans la somme (4) des coefficients non nuls. L'ensemble M étant fini, il y a un nombre naturel n satisfaisant aux conditions

$$a_{i_1\ldots i_m}\neq 0,\qquad i_1+\ldots+i_n=n$$

et

si $a_{k_1\ldots k_m}\neq 0$, alors $k_1+\ldots+k_m\leqslant n$ pour tout $(k_1, \ldots, k_m)\in M$.

Soit $M^*=\bigcup\limits_{k=0}^{n} S_k$. Posons

$$a_{(i)}=0 \text{ pour } (i)\in M^*\setminus M.$$

En s'appuyant sur (4), on conclut que

$$(5)\quad f=\sum_{(i)\in M^*} a_{(i)}x_1^{i_1}\dots x_m^{i_m}.$$

Comme $M^*=\bigcup\limits_{k=0}^{n} S_k$ et $S_l\cap S_k=\varnothing$ pour $l\neq k$. Il s'ensuit de (5) la représentation (2).

Admettons qu'outre la représentation (2) il existe une représentation (3). Si $m<n$, en soustrayant de l'égalité (2) l'égalité (3), il vient

$$(6)\quad \sum_{(i)\in S_n} a_{(i)}x_1^{i_1}\dots x_m^{i_m}+\ldots+\sum_{k=0}^{m}\Big(\sum_{(j)\in S_k}(a_{(j)}-b_{(j)})\,x_1^{j_1}\dots x_m^{j_m}\Big)=0.$$

En vertu de l'indépendance algébrique des éléments $x_1, \ldots, x_m$, tous les coefficients dans (6) sont nuls, et, en particulier,

$$a_{(i)}=0 \text{ pour tous } (i)\in S_n,$$

ce qui est en contradiction avec l'hypothèse du théorème. De façon analogue, on se convainc de l'impossibilité de l'inégalité $n < m$, donc $m = n$. Ainsi, l'égalité (6) peut être écrite sous forme

$$(7) \quad \sum_{k=0}^{n} \Big(\sum_{(j)\in S_k} (a_{(j)} - b_{(j)})\, x_1^{j_1} \ldots x_m^{j_m} \Big) = 0.$$

En vertu de l'indépendance algébrique de $x_1, \ldots, x_m$, il s'ensuit de (7) que $a_{(j)} = b_{(j)}$ pour tous les $(j) \in S_k$, où $k = \{0, 1, \ldots, n\}$. □

La représentation (2) du théorème 1.6 est appelée *représentation normale du polynôme.*

DÉFINITION. On appelle *degré du monôme* $a_{(i)}x_1^{i_1} \ldots x_m^{i_m}$, dont le coefficient $a_{(i)}$ n'est pas nul, la somme $i_1 + \ldots + i_m$.

DÉFINITION. On appelle *degré d'un polynôme f non nul*, $f \in K[x_1, \ldots, x_m]$ le plus grand des degrés des monômes non nuls entrant dans la représentation normale du polynôme f.

Le degré du polynôme nul n'est pas défini. Le degré du polynôme f est désigné par le symbole $\deg f$.

DÉFINITION. Un polynôme f de degré n est dit *homogène* si

$$f = \sum_{i_1 + \ldots + i_m = n} a_{(i)} x_1^{i_1} \ldots x_m^{i_m}.$$

Un polynôme homogène du premier degré est appelé *polynôme linéaire.*

Notons les propriétés les plus simples du degré d'un polynôme.

THÉORÈME 1.7. *Soient f et g deux polynômes quelconques de l'anneau des polynômes* $\mathcal{K}[x_1, \ldots, x_m]$. *On a alors:*

(1) *si* $f + g \neq 0$, *alors* $\deg (f + g) \leqslant \max \{\deg f, \deg g\}$;
(2) *si* $f \cdot g$ *est un polynôme non nul, alors* $\deg (fg) \leqslant \deg f + \deg g$;
(3) *si* $\mathcal{K}$ *est un domaine d'intégrité, alors* $\deg (fg) = \deg f + \deg g$.

La démonstration du théorème 1.7 est laissée au soin du lecteur.

Anneau de polynômes factoriel. Démontrons un théorème analogue au théorème 14.3.7.

THÉORÈME 1.8. *Soit* $\mathcal{K}$ *un anneau factoriel. Alors, l'anneau des polynômes* $\mathcal{K}[x_1, \ldots, x_n]$ *en* $x_1, \ldots, x_n$ *sur* $\mathcal{K}$ *est aussi un anneau factoriel.*

Démonstration. Le théorème se démontre par récurrence sur n. Pour $n = 1$ l'affirmation est vraie selon le théorème 14.3.7. Admettons que l'anneau des polynômes $\mathcal{K}[x_1, \ldots, x_{n-1}]$ en $x_1, \ldots, x_{n-1}$ sur $\mathcal{K}$ est factoriel. Démontrons qu'alors est également factoriel l'anneau $\mathcal{K}[x_1, \ldots, x_n]$. Selon le théorème 1.1,

$$\mathcal{K}[x_1, \ldots, x_n] = \mathcal{K}[x_1] \ldots [x_n] = (\mathcal{K}[x_1] \ldots [x_{n-1}])[x_n] = (\mathcal{K}[x_1, \ldots, x_{n-1}])[x_n].$$

Par hypothèse de récurrence, l'anneau $\mathcal{K}[x_1, \ldots, x_{n-1}]$ est factoriel. Par conséquent, en vertu du théorème 14.3.7, est factorielle son extension $(\mathcal{K}[x_1, \ldots, x_{n-1}])[x_n]$ par adjonction de l'élément x_n transcendant sur l'anneau $\mathcal{K}[x_1, \ldots, x_{n-1}]$. Ainsi, l'anneau des polynômes $\mathcal{K}[x_1, \ldots, x_n]$ est factoriel pour tout n naturel. □

COROLLAIRE 1.9. *Un anneau des polynômes* $\mathcal{F}[x_1, \ldots, x_n]$ *sur le corps* $\mathcal{F}$ *est factoriel.*

Exercices

1. Montrer que les polynômes suivants à deux variables sont irréductibles sur le corps des nombres rationnels: (a) $3x^2 - y$; (b) $x^2 + y^2 - 1$. Ces polynômes sont-ils réductibles sur un corps des nombres complexes?
2. Démontrer qu'un anneau des polynômes $\mathcal{F}[x, y]$ sur le corps $\mathcal{F}$ à deux variables ne constitue pas un anneau d'idéaux principaux.
3. Soit $\mathcal{F}[x, y]$ un anneau des polynômes sur le corps $\mathcal{F}$ à deux variables. Démontrer que l'anneau quotient $\mathcal{F}[x, y]/(x - y)$ est isomorphe à l'anneau $\mathcal{F}[x]$.

§ 2. Polynômes symétriques

Ordre lexicographique des termes d'un polynôme. Soient $\mathbf{N}$ un ensemble de tous les nombres naturels et m un nombre naturel fixé différent de zéro. Les éléments de l'ensemble $\mathbf{N}^m$ sont des vecteurs à m dimensions aux coordonnées naturelles. Soit

$$\mathbf{i} = (i_1, \ldots, i_m), \qquad \mathbf{k} = (k_1, \ldots, k_m).$$

Sur l'ensemble $\mathbf{N}^m$ introduisons un ordre lexicographique en estimant, par définition, que

$$(1) \quad (i_1, \ldots, i_m) < (k_1, \ldots, k_m)$$

si est positive la première coordonnée non nulle du vecteur $(k_1 - i_1, \ldots, k_m - i_m)$. On dira, en outre, que le vecteur $\mathbf{i}$ est inférieur au vecteur $\mathbf{k}$, tandis que le vecteur $\mathbf{k}$ est supérieur au vecteur $\mathbf{i}$.

THÉORÈME 2.1. *Un ordre lexicographique sur un ensemble* $\mathbf{N}^m$ *est une relation d'ordre linéaire strict.*

Démonstration. De la définition de l'ordre lexicographique il s'ensuit que pour deux vecteurs quelconques $\mathbf{i}, \mathbf{k}$ de $\mathbf{N}^m$ n'est satisfaite que l'une des trois conditions: $\mathbf{i} < \mathbf{k}$, $\mathbf{i} = \mathbf{k}$, $\mathbf{k} < \mathbf{i}$.

La relation $<$ sur l'ensemble $\mathbf{N}^m$ est transitive. De fait, si $\mathbf{i} < \mathbf{k}$ et $\mathbf{k} < \mathbf{l}$, alors $\mathbf{k} - \mathbf{i} > \mathbf{0}$, $\mathbf{l} - \mathbf{k} > \mathbf{0}$, où $\mathbf{0} = (0, \ldots, 0)$. Il s'ensuit que $(\mathbf{k} - \mathbf{i}) + (\mathbf{l} - \mathbf{k}) > \mathbf{0}$ et $\mathbf{l} - \mathbf{i} > \mathbf{0}$, c'est-à-dire $\mathbf{i} < \mathbf{l}$. □

COROLLAIRE 2.2. *Soit M un sous-ensemble fini non vide de l'ensemble* $\mathbf{N}^m$. *L'ordre lexicographique sur* $\mathbf{N}^m$ *induit donc un ordre linéaire strict sur M.*

Soient f un polynôme non nul de l'anneau des polynômes

$\mathscr{K}[x_1, \ldots, x_m]$ et

(2) $f = \sum_{(i) \in M} a_{(i)} x_1^{i_1} \ldots x_m^{i_m}$

sa représentation à coefficients non nuls, c'est-à-dire

$a_{(i)} \neq 0$ pour chaque $(i) \in M$.

Soit S un ensemble de monômes figurant dans f (dans la somme (2)). Introduisons sur l'ensemble S la relation d'ordre en posant que

(3) $a_{i_1 \ldots i_m} x_1^{i_1} \ldots x_m^{i_m} < a_{k_1 \ldots k_m} x_1^{k_1} \ldots x_m^{k_m}$

si et seulement si $(i_1, \ldots, i_m) < (k_1, \ldots, k_m)$. En effet, cette relation binaire est transitive, antiréflexive et, de plus, linéaire. Donc, la relation d'ordre lexicographique sur S est aussi un ordre linéaire strict.

DÉFINITION. Le plus grand élément d'un ensemble ordonné $\langle S, <\rangle$ est appelé *terme directeur du polynôme* f.

Si l'inégalité (3) est remplie, on dit que le terme $a_{i_1 \ldots i_m} x_1^{i_1} \ldots x_m^{i_m}$ est inférieur au terme $a_{k_1 \ldots k_m} x_1^{k_1} \ldots x_m^{k_m}$. Le terme directeur est évidemment supérieur à tout autre monôme du polynôme f.

Lemme sur le terme directeur du produit de deux polynômes. Lors de l'étude des propriétés des polynômes symétriques le lemme suivant s'avère nécessaire.

LEMME 2.3. *Soit* $\mathscr{K}[x_1, \ldots, x_m]$ *un anneau des polynômes en* $x_1, \ldots, x_m$ *sur le domaine d'intégrité* $\mathscr{K}$. *Le terme directeur du produit de deux polynômes non nuls de l'anneau* $\mathscr{K}[x_1, \ldots, x_m]$ *est égal au produit des termes directeurs des cofacteurs.*

Démonstration. Soient f et g des polynômes non nuls de l'anneau considéré, $ax_1^{i_1} \ldots x_m^{i_m}$ et $bx_1^{k_1} \ldots x_m^{k_m}$ les termes directeurs des polynômes f et g respectivement. Il faut démontrer que le terme directeur du polynôme fg est le monôme

(I) $abx_1^{i_1+k_1} \ldots x_m^{i_m+k_m}$.

Notons que $ab \neq 0$, car $\mathscr{K}$ est un domaine d'intégrité. Soient

(1) $cx_1^{j_1} \ldots x_m^{j_m}$ et $dx_1^{s_1} \ldots x_m^{s_m}$

tous termes non nuls en représentations normales des polynômes f et g respectivement. On a alors les inégalités

(2) $(j_1, \ldots, j_m) \leqslant (i_1, \ldots, i_m)$,

(3) $(s_1, \ldots, s_m) \leqslant (k_1, \ldots, k_m)$.

Il nous suffit de montrer que si une au moins de ces inégalités est stricte, alors

(4) $cdx_1^{j_1+s_1} \ldots x_m^{j_m+s_m} < abx_1^{i_1+k_1} \ldots x_m^{i_m+k_m}$.

En effet, si une au moins des inégalités (2) et (3) est stricte, on a

(5) $(i_1 - j_1, \ldots, i_m - j_m) > 0$ ou $(k_1 - s_1, \ldots, k_m - s_m) > 0$

et, en vertu de (2), (3), (5), il vient

(6) $(i_1 + k_1, \ldots, i_m + k_m) - (j_1 + s_1, \ldots, j_m + s_m) > 0$.

De (6) on déduit (4). L'inégalité (4) est remplie pour tous termes non nuls de (1) en représentations normales des polynômes f et g dont l'un au moins n'est pas le terme directeur du polynôme respectif. Sur la base de ces raisonnements on conclut que le monôme (I) est le terme directeur du produit fg. □

Polynômes symétriques. Soit $\mathcal{K}[x_1, \ldots, x_m]$ un anneau des polynômes en $x_1, \ldots, x_m$ sur l'anneau commutatif $\mathcal{K}$. Soit S_m un ensemble de permutations de degré m.

DÉFINITION. Un polynôme f de $\mathcal{K}[x_1, \ldots, x_m]$ est dit *polynôme symétrique en* $x_1, \ldots, x_m$ si pour toute permutation $\tau \in S_m$ on a l'égalité

$$f(x_1, \ldots, x_m) = f(x_{\tau(1)}, \ldots, x_{\tau(m)}).$$

E x e m p l e. Le polynôme $x_1^2 + \ldots + x_m^2 + x_1 + x_2 + \ldots + x_m$ redevient lui-même pour toute permutation des éléments $x_1, \ldots, x_m$.

DÉFINITION. On appelle *polynômes symétriques élémentaires en* $x_1, \ldots, x_m$ les polynômes

$$\sigma_1 = x_1 + x_2 + \ldots + x_m;$$
$$\sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_{m-1}x_m;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\sigma_m = x_1x_2 \ldots x_m.$$

Ils apparaissent tout naturellement avec l'étude du polynôme $\varphi = (z - x_1)(z - x_2) \ldots (z - x_m)$ égal au polynôme

$$z^m - (x_1 + x_2 + \ldots + x_m) z^{m-1} + \\ + (x_1x_2 + \ldots + x_{m-1}x_m) z^{m-2} + \ldots + (-1)^m x_1 \ldots x_m.$$

Ainsi, $\varphi = z^m - \sigma_1 z^{m-1} + \sigma_2 z^{m-2} - \ldots + (-1)^m \sigma_m$.

On vérifie sans peine que l'ensemble de tous les polynômes symétriques de l'anneau $\mathcal{K}[x_1, \ldots, x_m]$ est un sous-anneau de cet anneau; notons-le $S\mathcal{K}[x_1, \ldots, x_m]$. D'autre part les polynômes symétriques élémentaires en $x_1, \ldots, x_m$ engendrent un certain sous-anneau $\mathcal{K}[x_1, \ldots, x_m]$ qu'on notera $\mathcal{K}[\sigma_1, \ldots, \sigma_m]$. On

constate aisément que

$$\mathcal{K}\,[\sigma_1, \ldots, \sigma_m] \subset S\mathcal{K}\,[x_1, \ldots, x_m].$$

Ces deux anneaux coïncident-ils? Tout polynôme symétrique en $x_1, \ldots, x_m$ est-il représentable sous forme de polynôme composé de polynômes symétriques élémentaires $\sigma_1, \ldots, \sigma_m$? On donnera plus loin une réponse affirmative à cette question.

Lemmes des polynômes symétriques. Soit $\mathcal{K}\,[x_1, \ldots, x_m]$ un anneau des polynômes en $x_1, \ldots, x_m$.

LEMME 2.4. *Si $ax_1^{k_1}x_2^{k_2} \ldots x_m^{k_m}$ est le terme directeur d'un polynôme symétrique, alors $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_m$.*

Démonstration. Soient f un polynôme de $K\,[x_1, \ldots, x_m]$ symétrique par rapport à $x_1, \ldots, x_m$, et

$$(1) \quad ax_1^{k_1}x_2^{k_2} \ldots x_m^{k_m} \quad (a \in K)$$

le terme directeur du polynôme f. La représentation normale du polynôme symétrique f comporte également les monômes

$$(2) \quad ax_1^{k_2}x_2^{k_1}x_3^{k_3} \ldots x_m^{k_m},$$

$$(3) \quad ax_1^{k_1}x_2^{k_3}x_3^{k_2} \ldots x_m^{k_m}.$$

Vu que le monôme (1) est supérieur au monôme (2), on a $k_1 \geqslant k_2$. Puisque le monôme (1) est supérieur au monôme (3), on a $k_2 \geqslant k_3$, etc. Par conséquent, $k_1 \geqslant k_2 \geqslant k_3 \geqslant \ldots \geqslant k_m$. □

LEMME 2.5. *Soit $ax_1^{k_1}x_2^{k_2} \ldots x_m^{k_m}$ le terme directeur d'un polynôme symétrique non nul $f \in K\,[x_1, \ldots, x_m]$. Alors les termes directeurs des polynômes f et $a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3} \ldots \sigma_m^{k_m}$ coïncideront.*

Démonstration. On voit aisément que les polynômes symétriques élémentaires $\sigma_1, \sigma_2, \ldots, \sigma_{m-1}, \sigma_m$ sont munis des termes directeurs suivants:

$$x_1, \; x_1x_2, \; \ldots, \; x_1x_2 \ldots x_{m-1}, \; x_1x_2 \ldots x_m.$$

Selon le lemme sur le terme directeur du produit des polynômes les termes directeurs des polynômes

$$(1) \quad a\sigma_1^{k_1-k_2}, \; \sigma_2^{k_2-k_3}, \; \ldots, \; \sigma_{m-1}^{k_{m-1}-k_m}, \; \sigma_m^{k_m}$$

sont respectivement les monômes

$$ax_1^{k_1-k_2}, \; (x_1x_2)^{k_2-k_3}, \; \ldots, \; (x_1x_2 \ldots x_{m-1})^{k_{m-1}-k_m}, \; (x_1 \ldots x_m)^{k_m}.$$

En vertu du même lemme, le produit de ces monômes, c'est-à-dire le monôme $ax_1^{k_1}x_2^{k_2} \ldots x_m^{k_m}$ est le terme directeur du produit des polynômes (1). Ainsi, les termes directeurs des polynômes f et $a\sigma_1^{k_1-k_2}, \ldots, \sigma_m^{k_m}$ coïncident. □

Soit $\mathcal{K}\,[x_1, \ldots, x_m]$ un anneau des polynômes en $x_1, \ldots, x_m$. Introduisons sur l'ensemble des polynômes non nuls de cet anneau

la relation binaire $>$: $f > g$ *si et seulement si le terme directeur de f est supérieur à celui de g.* On constate sans peine que cette relation est de nature linéaire.

DÉFINITION. La suite $\varphi_1, \varphi_2, \varphi_3, \ldots$ de polynômes de $K[x_1, \ldots, x_n]$ est appelée *chaîne descendante* si

(1) $\varphi_1 > \varphi_2 > \varphi_3 > \ldots$

LEMME 2.6. *Une chaîne descendante de polynômes symétriques non nuls de l'anneau des polynômes $\mathcal{K}[x_1, \ldots, x_m]$ ne peut être infinie.*

Démonstration. Soit (1) une chaîne descendante de polynômes symétriques. Le terme directeur φ_i est alors supérieur au terme directeur φ_{i+1} pour $i = 1, 2, 3, \ldots$ Soit $ax_1^{k_1}x_2^{k_2} \ldots x_m^{k_m}$ le terme directeur du polynôme φ_1. φ_1 étant symétrique, il s'ensuit du lemme 2.4 que $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_m$. Soit $(l_1, l_2, \ldots, l_m)$ le vecteur des indices du terme directeur d'un polynôme symétrique quelconque φ_i de la chaîne (1) différent de φ_1. En vertu de (1),

$$(k_1, k_2, \ldots, k_m) > (l_1, l_2, \ldots, l_m),$$

donc,

(2) $k_1 \geqslant l_1 \geqslant l_2 \geqslant \ldots \geqslant l_m$.

Substituons à ces conditions des conditions moins strictes

(3) $0 \leqslant l_1 \leqslant k_1, \ldots, 0 \leqslant l_m \leqslant k_1$.

Le nombre de vecteurs $(l_1, \ldots, l_m)$ de $\mathbf{N}^m$ satisfaisant aux conditions (3) pour un k_1 fixé est apparemment fini et vaut $(k_1 + 1)^m$. Aussi le nombre de vecteurs $(l_1, \ldots, l_m)$ satisfaisant aux conditions (2) est-il également fini, car des conditions (2) se déduisent les conditions (3). Par conséquent, la chaîne (3) ne peut être infinie. □

Théorème fondamental des polynômes symétriques. Soit $\mathcal{K}[x_1, \ldots, x_m]$ un anneau de polynômes en $x_1, \ldots, x_m$ sur un domaine d'intégrité $\mathcal{K}$. Soient $\sigma_1, \ldots, \sigma_m$ des polynômes symétriques en $x_1, \ldots, x_m$. Tout polynôme $g(\sigma_1, \ldots, \sigma_m)$ sur $\mathcal{K}$ sera considéré comme un polynôme symétrique

$$g(\sigma_1(x_1, \ldots, x_m), \ldots, \sigma_m(x_1, \ldots, x_m)) \text{ en } x_1, \ldots, x_m \text{ sur } \mathcal{K}.$$

THÉORÈME 2.7. *Tout polynôme symétrique de l'anneau des polynômes $\mathcal{K}[x_1, \ldots, x_m]$ peut se représenter sous forme d'un polynôme sur $\mathcal{K}$ composé de polynômes symétriques élémentaires $\sigma_1, \ldots, \sigma_m$, c'est-à-dire que pour tout $f(x_1, \ldots, x_m) \in K[x_1, \ldots, x_m]$ il existe un polynôme $g(x_1, \ldots, x_m) \in \mathcal{K}[x_1, \ldots, x_m]$ tel que*

$$f(x_1, \ldots, x_m) = g(\sigma_1(x_1, \ldots, x_m), \ldots, \sigma_m(x_1, \ldots, x_m)).$$

Démonstration. Soient f un polynôme symétrique non nul sur $\mathcal{K}$ et $a_0x_1^{k_1} \ldots x_m^{k_m}$ son terme directeur. Le polynôme

(1) $f_1 = f - a_0\sigma^{k_1-k_2} \ldots \sigma_m^{k_m}$

est symétrique, vu que c'est une différence de polynômes symétriques, de plus, selon le lemme 2.5, $f > f_1$. Soit $a_1 x_1^{l_1} \ldots x_m^{l_m}$ le terme directeur du polynôme f_1. De façon analogue,

(2) $f_2 = f_1 - a_1 \sigma^{l_1 - l_2} \ldots \sigma_m^{l_m}$

est un polynôme symétrique, avec $f_1 > f_2$, etc. On obtient finalement une chaîne descendante de polynômes symétriques $f_0 > f_1 > > f_2 > \ldots$ Selon le lemme 2.6 cette chaîne ne peut être infinie. Supposons qu'elle s'arrête à $(s+1)$-ième étape, c'est-à-dire

$(s+1)$ $f_{s+1} = f_s - a_s \sigma_1^{n_1 - n_2} \ldots \sigma_m^{n_m} = 0.$

En sommant terme à terme les égalités (1), (2), . . , $(s+1)$, il vient

$$f = a_0 \sigma^{k_1 - k_2} \ldots \sigma_m^{k_m} + a_1 \sigma_1^{l_1 - l_2} \ldots \sigma_m^{l_m} + \ldots + a_s \sigma_1^{n_1 - n_m} \ldots \sigma_m^{n_m}.$$

Cette égalité fournit la représentation cherchée du polynôme symétrique f sous forme d'un polynôme sur $\mathcal{K}$ composé des polynômes symétriques élémentaires $\sigma_1, \ldots, \sigma_m$. □

Exemple. $x_1^2 + x_2^2 + \ldots + x_m^2 = (x_1 + \ldots + x_m)^2 - 2(x_1 x_2 + \ldots + x_{m-1} x_m) = \sigma_1^2 - 2\sigma_2$.

COROLLAIRE 2.8. *Soient* $\varphi = z^m + a_1 z^{m-1} + \ldots + a_m$ *un polynôme sur un anneau numérique* $\mathcal{K}$ *et* $\varphi = (z - c_1)(z - c_2) \ldots \ldots (z - c_m)$, *où* $c_1, \ldots, c_m \in \mathbf{C}$. *Si* $f(x_1, \ldots, x_m)$ *est un polynôme symétrique en* $x_1, \ldots, x_m$ *avec coefficients dans* K, *alors* $f(c_1, \ldots, c_m) \in K$.

Démonstration. De l'égalité

$$(z - c_1)(z - c_2) \ldots (z - c_m) = z^m + a_1 z^{m-1} + a_2 z^{m-2} + \ldots \ldots + a_m$$

s'ensuivent les formules suivantes (de *Viète*) exprimant la relation liant les racines et les coefficients du polynôme

$$c_1 + \ldots + c_m = -a_1;$$
$$c_1 c_2 + \ldots + c_{m-1} c_m = a_2;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$c_1 c_2 \ldots c_m = (-1)^m a_m.$$

Ces égalités peuvent être écrites sous forme

$$(1) \quad \begin{aligned} &\sigma_1(c_1, \ldots, c_m) = -a_1; \\ &\sigma_2(c_1, \ldots, c_m) = a_2; \\ &\ldots\ldots\ldots\ldots\ldots \\ &\sigma_m(c_1, \ldots, c_m) = (-1)^m a_m. \end{aligned}$$

En vertu du théorème fondamental des polynômes symétriques, le polynôme f de $K[x_1, \ldots, x_m]$ peut être représenté sous forme d'un

polynôme g composé de polynômes symétriques élémentaires $\sigma_1, \ldots$ $\ldots, \sigma_m$ avec coefficients dans K, c'est-à-dire

(2) $f(x_1, \ldots, x_m) = g(\sigma_1(x_1, \ldots, x_m), \ldots, \sigma_m(x_1, \ldots, x_m))$.

En posant dans l'égalité (2) $x_1 = c_1, \ldots, x_m = c_m$ et, compte tenu de l'égalité (1), il vient

(3) $f(c_1, \ldots, c_m) = g(-a_1, a_2, \ldots, (-1)^m a_m)$.

De plus, $g \in K[x_1, \ldots, x_m]$ et $a_1, \ldots, a_m \in K$, par conséquent, $f(c_1, \ldots, c_m) \in K$. □

Exercices

1. Le polynôme $(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ peut-il être considéré comme un polynôme symétrique?

2. Chercher le terme directeur du polynôme $2\sigma_1^4\sigma_2^3\sigma_3^3$, où $\sigma_1 = x_1 + x_2 + x_3$, $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$, $\sigma_3 = x_1x_2x_3$.

3. Montrer que l'ensemble de tous les polynômes symétriques de $K[x_1, \ldots, x_n]$, où K est l'ensemble de base du domaine d'intégrité $\mathscr{K}$, est fermé dans l'anneau des polynômes $\mathscr{K}[x_1, \ldots, x_n]$.

4. Chercher la somme des cubes des racines complexes du polynôme $2z^4 - 4z^3 + 2z^2 - 6z + 1$.

5. Chercher la somme des carrés des racines complexes du polynôme $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ sur le corps des nombres complexes.

§ 3. Résultant des polynômes et élimination des variables

Résultant de deux polynômes. Soient f et g des polynômes de l'anneau des polynômes $\mathscr{F}[x]$ sur le corps $\mathscr{F}$. Cherchons les conditions pour lesquelles ces polynômes possèdent un diviseur commun de puissance positive.

THÉORÈME 3.1. *Soient f et g des polynômes en x sur le corps $\mathscr{F}$ tels que*

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_n,$$
$$g = b_0x^m + b_1x^{m-1} + \ldots + b_m,$$

dont un au moins des coefficients a_0, b_0 est différent de zéro. Les polynômes f et g possèdent un diviseur commun de puissance positive dans $\mathscr{F}[x]$ si et seulement s'il existe dans $F[x]$ des polynômes c et d satisfaisant aux conditions:

(α) $fc = gd$,

(β) $c = c_0x^{m-1} + \ldots + c_{m-1}$, $d = d_0x^{n-1} + \ldots + d_{n-1}$,

(γ) *un au moins des polynômes c et d est différent de zéro.*

DÉMONSTRATION. Supposons que les polynômes f et g possèdent dans $F[x]$ un diviseur commun u de puissance positive. Il existe

alors des polynômes c et d tels que $f = du$, $g = cu$. On vérifie sans peine que les polynômes c et d satisfont aux conditions (α)-(γ).

Supposons à présent qu'il existe des polynômes c, d satisfaisant aux conditions (α), (β) et (γ). Posons que le degré du polynôme f vaut n, c'est-à-dire $a_0 \neq 0$ (dans le cas contraire on pourrait intervertir les rôles de f et g). Soit φ le plus grand commun diviseur de c et d. Alors dans $F[x]$ on trouve des polynômes c_1 et d_1 tels que

(1) $\quad c = c_1\varphi, \quad d = d_1\varphi, \quad \text{PGCD}\,(c_1, d_1) = 1.$

Notons que $d_1 \neq 0$, car dans le cas contraire $d = 0$ et, en raison de (α), $c = 0$, ce qui est en contradiction avec la condition (γ). En vertu de (1) et de la condition (α), $fc_1\varphi = gd_1\varphi$ et, par suite,

(2) $\quad fc_1 = gd_1.$

Le polynôme d_1 divisant fc_1 et étant premier avec c_1, d_1 divise f; de sorte que

(3) $\quad f = d_1t,$

où t est un polynôme de degré positif, vu que le degré de d_1 n'est pas supérieur au degré de d, tandis que le degré de d est inférieur au degré de f, en vertu de la condition (β). De (3) et (2) on déduit $d_1th = gd_1$ et $g = ht$. Ainsi, f et g possèdent un diviseur commun t de puissance positive. □

Ecrivons les conditions (α) et (β) en plus de détails:

(1) $$(a_0x^n + \ldots + a_n)(c_0x^{m-1} + \ldots + c_{m-1}) = (b_0x^m + \ldots + b_m)(d_0x^{n-1} + \ldots + d_{n-1}).$$

Après avoir effectué la multiplication dans les deux membres de l'égalité et égalé les coefficients des mêmes puissances de x, on aboutit au système suivant d'équations linéaires

$$\begin{aligned}
a_0c_0 &= b_0d_0;\\
a_1c_0 + a_0c_1 &= b_1d_0 + b_0d_1;\\
a_2c_0 + a_1c_1 + a_0c_2 &= b_2d_0 + b_1d_1 + b_0d_2;\\
&\ldots\ldots\ldots\ldots\\
a_nc_{m-2} + a_{n-1}c_{m-1} &= b_md_{n-2} + b_{m-1}d_{n-1};\\
a_nc_{m-1} &= b_md_{n-1}.
\end{aligned}$$

C'est un système de $n + m$ équations linéaires homogènes à $n + m$ variables $c_0, c_1, \ldots, c_{m-1}, d_0, d_1, \ldots, d_{n-1}$. Il possède des solutions non nulles si et seulement si le déterminant de ce système est nul. Pour éviter l'apparition des moins devant les éléments de la matrice du déterminant, on peut faire passer les seconds membres dans les premiers et considérer comme variables $c_0, c_1, \ldots, c_{m-1}$, $-d_0, -d_1, \ldots, -d_{n-1}$. Si, de plus, on transpose la matrice du dé-

terminant, ce dernier prend la forme

$$R = \begin{vmatrix} a_0 & a_1 & \dots & a_n & & & \\ & a_0 & a_1 & \dots & a_n & & \\ & & \dots & \dots & \dots & \dots & \\ & & & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & b_m & & & \\ & b_0 & b_1 & \dots & b_m & & \\ & & \dots & \dots & \dots & \dots & \\ & & & b_0 & b_1 & \dots & b_m \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \end{matrix}$$

DÉFINITION. On appelle résultant des polynômes $f = a_0x^n + \dots$ $\dots + a_n$ et $g = b_0x^m + \dots + b_m$ le *déterminant* R.

Il s'ensuit du théorème 3.1 que les polynômes f et g (où $a_0 \neq 0$ ou $b_0 \neq 0$) admettent un diviseur commun de puissance positive si et seulement si le système d'équations linéaires possède des solutions non nulles, c'est-à-dire quand le déterminant R est nul. Bref, on a démontré le théorème suivant.

THÉORÈME 3.2. *Soient* $f = a_0x^n + \dots + a_n$, $g = b_0x^m + \dots$ $\dots + b_m$ *des polynômes sur le corps* $\mathscr{F}$ *et un au moins des coefficients* a_0 *et* b_0 *n'est pas nul. Les polynômes* f *et* g *possèdent un diviseur commun de puissance positive si et seulement si le résultant de ces polynômes vaut zéro.*

COROLLAIRE 3.3. *Si le résultant des polynômes* f *et* g *est nul, alors les polynômes soit possèdent un diviseur commun de puissance positive, soit les coefficients* a_0 *et* b_0 *sont nuls, et réciproquement.*

Elimination des variables. On peut appliquer le résultant pour éliminer les variables du système de deux équations algébriques dont l'une au moins n'est pas linéaire et possède deux variables. Soit donné un système d'équations

(1) $f(x, y) = 0, \qquad g(x, y) = 0,$

où f et g sont des polynômes en x et y sur le corps $\mathscr{F}$. Ecrivons ces polynômes suivant les puissances décroissantes de x,

$$f(x, y) = a_0(y)x^n + a_1(y)x^{n-1} + \dots + a_n(y);$$
$$g(x, y) = b_0(y)x^m + b_1(y)x^{m-1} + \dots + b_n(y),$$

où $a_i(y)$ et $b_k(y)$ sont des polynômes de l'anneau $\mathscr{F}[y]$. Cherchons le résultant des polynômes f et g en les considérant comme des polynômes en x. Ce résultant est un polynôme de l'anneau $\mathscr{F}[y]$ qu'on notera $R(y)$.

Supposons que le système (1) admet dans le corps $\mathscr{F}$ (ou dans son extension) une solution (α, β). Dans ce cas les polynômes

$$f(x, \beta) = a_0(\beta)x^n + a_1(\beta)x^{n-1} + \dots + a_n(\beta);$$
$$g(x, \beta) = b_0(\beta)x^m + b_1(\beta)x^{m-1} + \dots + b_m(\beta)$$

ont une même racine α. Ils ont donc un multiple commun de puissance positive (sur $F(\beta)$). Par conséquent, en vertu du théorème 3.2, leur résultant égal à $R(\beta)$ devrait être égal à zéro. Réciproquement : si β est une racine du résultant $R(y)$, c'est-à-dire $R(\beta) = 0$, alors, selon le corollaire 3.3, les polynômes $f(x, \beta)$ et $g(x, \beta)$ possèdent soit une racine commune, soit leurs coefficients $a_0(\beta)$ et $b_0(\beta)$ sont tous les deux nuls.

Ainsi, la résolution du système d'équations (1) à deux variables se réduit à la résolution de l'équation

(2) $R(y) = 0$

à une variable y. On dit que l'équation (2) est le résultant de l'élimination de x du système d'équations (1).

Exemple. Cherchons les solutions du système d'équations

$$(1)\quad \begin{aligned} &x^2y^2 + x^2y + y + x = 0,\\ &xy^2 + 2xy + 1 = 0.\end{aligned}$$

Eliminons x du système (1). Pour ce faire écrivons les premiers membres des équations suivant les puissances décroissantes de x:

$$(2')\quad \begin{aligned} &(y^2 + y)\,x^2 + x + y = 0,\\ &(y^2 + 2y)\,x + 1 = 0\end{aligned}$$

et composons le déterminant :

$$R(y) = \begin{vmatrix} y^2+y & 1 & y \\ y^2+2y & 1 & 0 \\ 0 & y^2+2y & 1 \end{vmatrix}.$$

En calculant le déterminant, on obtient

$$R(y) = y^2 + y + y(y^2 + 2y)^2 - y^2 - 2y = \\ = y[(y^2 + 2y)^2 - 1].$$

L'équation $R(y) = y[(y^2 + 2y)^2 - 1] = y(y + 1)^2(y^2 + 2y) - 1)$ présente des racines $0, -1, -1 + \sqrt{2}, -1 - \sqrt{2}$.

Pour $y = 0$ le système (1) se transforme en système $x = 0$, $1 = 0$, qui est incompatible.

Pour $y = -1$ le système (1) se transforme en système $x - 1 = 0$, $-x + 1 = 0$. Ainsi, on obtient la solution du système (1) : $(1, -1)$.

Pour $y = -1 \pm \sqrt{2}$ le système (1) se transforme en système

$$\begin{aligned} &(2 \mp \sqrt{2})\,x^2 + x + (-1 \pm \sqrt{2}) = 0,\\ &x + 1 = 0,\end{aligned}$$

dont la solution est $x = -1$. On obtient, par conséquent, encore deux solutions du système (1) : $(-1, -1 + \sqrt{2})$, $(-1, -1 - \sqrt{2})$.

Exercices

1. Calculer le résultant des polynômes:

(a) $2x^3 - 3x^2 + 2x + 1$ et $x^2 + x + 3$;

(b) $x^3 + 2x^2 + 2x - 2$ et $x^2 - 2x + 4$;

(c) $x^3 - 3x + 6$ et $x^3 + x^2 - x - 1$.

2. Pour quelle valeur de λ les polynômes possèdent une racine commune:

(a) $x^3 - 2\lambda x + \lambda^3$ et $x^2 + \lambda^2 - 2$;

(b) $x^3 + \lambda x^2 - 9$ et $x^2 + \lambda x - 3$?

3. Eliminer x du système d'équations

$x^2 - 3xy + y^2 - 2 = 0, \quad 2x^2 - xy + 3y^2 - 1 = 0.$

4. En utilisant le résultant résoudre le système d'équations

$y^2 + x^2 - y - 3x = 0, \quad y^2 - 6xy - x^2 + 11y + 7x - 12 = 0.$

CHAPITRE XVI

POLYNÔMES SUR UN CORPS DES NOMBRES COMPLEXES ET SUR UN CORPS DES NOMBRES RÉELS

§ 1. Corps des nombres complexes algébriquement fermé

Théorème de l'accroissement du module d'un polynôme. Soient $\mathscr{C}[z]$ un anneau des polynômes sur un corps des nombres complexes $\mathscr{C}$ et $\mathbf{C}[z]$ son ensemble de base.

THÉORÈME 1.1. *Soit f un polynôme de degré positif de* $\mathbf{C}[z]$. *Pour tout nombre réel $M > 0$, il existe un nombre réel $r > 0$ tel que pour tout nombre complexe z $|f(z)| \geqslant M$, aussitôt que $|z| \geqslant r$.*

Démonstration. Soient

$$f(z) = a_0 + a_1 z + \ldots + a_n z^n \in \mathbf{C}[z], \quad a_n \neq 0, \quad n \geqslant 1.$$

En vertu des propriétés du module (théorème 4.7.8),

$$|a_n z^n + a_{n-1} z^{n-1} + \ldots + a_0| \geqslant |a_n z^n| - |a_0 + a_1 z + \ldots + a_{n-1} z^{n-1}|,$$
$$|a_0 + a_1 z + \ldots + a_{n-1} z^{n-1}| \leqslant |a_0| + |a_1|\,|z| + \ldots + |a_{n-1}|\,|z|^{n-1}.$$

Par conséquent, pour $z \neq 0$

$$(1) \quad |f(z)| \geqslant |a_n|\,|z|^n \left[1 - \left(\frac{|a_0|}{|a_n|\,|z|^n} + \ldots + \frac{|a_{n-1}|}{|a_n|\,|z|}\right)\right].$$

Posons

$$(2) \quad b = \max\left\{\frac{|a_0|}{|a_n|}, \ \ldots, \ \frac{|a_{n-1}|}{|a_n|}\right\}.$$

Notons que pour $k \geqslant 1$ et $|z| \geqslant 1$ les inégalités $|z|^k \geqslant |z|$ et

$$(3) \quad \frac{1}{|z|^k} \leqslant \frac{1}{|z|}$$

sont remplies. Sur la base de (1)-(3), il vient

$$(4) \quad |f(z)| \geqslant |a_n|\,|z|^n \left(1 - \frac{nb}{|z|}\right).$$

On voit sans peine que

$$(5) \quad \left(1 - \frac{nb}{|z|}\right) \geqslant \frac{1}{2} \quad \text{si } |z| \geqslant 2nb.$$

Ensuite, on a

(6) $\frac{|a_n|\,|z|^n}{2} \geqslant M$, si $|z| \geqslant \left(\frac{2M}{|a_n|}\right)^{1/n}$.

Sur la base de (4)-(6), on conclut que

$$|f(z)| \geqslant M, \text{ si } |z| \geqslant r,$$

où $r = \max\left\{1,\ 2nb,\ \left(\frac{2M}{|a_n|}\right)^{1/n}\right\}$. □

Continuité du module d'un polynôme. Soit f un polynôme en z sur le corps des nombres complexes. L'application $z \mapsto |f(z)|$ définie sur l'ensemble **C** de tous les nombres complexes est une fonction réelle de la variable complexe. On l'appellera *module du polynôme* f en le désignant par le symbole $|f|$.

Théorème 1.2. *Soit f un polynôme quelconque de* **C** [z]. *Le module du polynôme f est une fonction continue sur l'ensemble* **C**.

Démonstration. Montrons que pour tout ε positif il existe un δ positif tel que pour tout nombre complexe z si $|z - a| < \delta$, alors $||f(z)| - |f(a)|| < \varepsilon$.

Le théorème est apparemment vrai si le polynôme f est nul ou de degré zéro. Supposons que le polynôme f est de degré n positif.

Décomposons f en puissances de la différence $z - a$:

$$f(z) = c_0 + c_1(z - a) + \ldots + c_n(z - a)^n \qquad (c_n \neq 0).$$

Comme $f(a) = c_0$, il vient

$$f(z) - f(a) = c_1(z - a) + \ldots + c_n(z - a)^n$$

et, selon le théorème 4.7.8, s'ensuit l'inégalité

(1) $|f(z) - f(a)| \leqslant |c_1|\,|z - a| + \ldots + |c_n|\,|z - a|^n$.

Posons

$$b = \max\{|c_1|, \ldots, |c_n|\};$$

comme $c_n \neq 0$, $b \neq 0$. On voit sans peine que pour $k \geqslant 1$, il vient

(2) $|z - a|^k \leqslant |z - a|$ si $|z - a| \leqslant 1$.

En vertu de (1) et (2), on a

$$|f(z) - f(a)| \leqslant nb\,|z - a|.$$

En outre, pour tout $\varepsilon > 0$

$$nb\,|z - a| < \varepsilon, \text{ si } |z - a| < \varepsilon/nb.$$

Associons à chaque nombre ε un δ positif tel que $\delta = \min\left\{\frac{\varepsilon}{nb}, 1\right\}$; alors $|f(z) - f(a)| < \varepsilon$ si $|z - a| < \delta$. En outre, pour tout nombre complexe z

$$||f(z)| - |f(a)|| \leqslant |f(z) - f(a)|.$$

Par conséquent, pour tout $\varepsilon > 0$ il existe un $\delta > 0$ tel que pour tout z de **C**, on ait

$$||f(z)| - |f(a)|| < \varepsilon \text{ si } |z - a| < \delta. \ \square$$

THÉORÈME 1.3. *Soit f un polynôme de* **C** [z]. *Si la suite* $\langle z_n \rangle$ *converge vers un nombre complexe a, alors la suite* $\langle |f(z_n)| \rangle$ *converge vers le nombre* $|f(a)|$.

Démonstration. Selon le théorème 1.2,

$$(1) \quad (\forall \varepsilon > 0)(\exists \delta > 0)(\forall z \in \mathbf{C})(|z - a| < \delta \to \to ||f(z)| - |f(a)|| < \varepsilon).$$

Par hypothèse, la suite $\langle z_n \rangle$ converge vers le nombre a. Donc, pour tout $\delta > 0$ il existe un nombre naturel n_0 tel que $|z_n - a| < \delta$ avec $n > n_0$ quelconque. De là, en vertu du (1), s'ensuit

$$(\forall \varepsilon > 0)(\exists n_0 \in \mathbf{N})(\forall n \in \mathbf{N})(n > n_0 \to \to ||f(z_n)| - |f(a)|| < \varepsilon).$$

Ainsi, la suite $\langle |f(z_n)| \rangle$ converge vers le nombre $|f(a)|$. $\square$

Valeur minimale du module d'un polynôme. Pour l'exposé ultérieur on aura besoin du théorème de Bolzano-Weierstrass connu de l'analyse: de toute suite infinie $\langle z_n \rangle$ de points du cercle $|z| \leqslant r$ (r étant un nombre réel positif fixé) on peut extraire une sous-suite convergeant en un certain point du cercle.

THÉORÈME 1.4. *Soient f un polynôme de* **C** [z], *r un nombre réel positif et* $m = \inf\limits_{|z| \leqslant r} |f(z)|$. *Alors, il existe un nombre complexe a tel que* $|f(a)| = m$ *et* $|a| \leqslant r$.

Démonstration. Soit $\langle \varepsilon_n \rangle$ une suite des nombres réels positifs convergeant vers zéro. Comme $m = \inf\limits_{|z| \leqslant r} |f(z)|$, il existe pour chaque terme ε_n de la suite un z_n vérifiant

$$(1) \quad m \leqslant |f(z_n)| \leqslant m + \varepsilon_n, \quad |z_n| \leqslant r.$$

Aussi la suite $\langle |f(z_n)| \rangle$ converge-t-elle vers m:

$$(2) \quad \lim_{n \to \infty} |f(z_n)| = m.$$

En vertu de (1), tous les éléments de la suite $\langle z_n \rangle$ appartiennent au cercle $|z| \leqslant r$. Selon le théorème de Bolzano-Weierstrass cette suite engendre une sous-suite $\langle x_n \rangle$ qui converge en un certain point a du cercle $|z| \leqslant r$, c'est-à-dire

$$(3) \quad \lim_{n \to \infty} x_n = a, \quad |a| \leqslant r.$$

Selon le théorème 1.3, de (3) s'ensuit

$$(4) \quad \lim_{n \to \infty} |f(x_n)| = |f(a)|.$$

Vu que $\langle |f(x_n)| \rangle$ est une sous-suite de la suite $\langle f(z_n) \rangle$ convergeant vers m, on a

(5) $$\lim_{n\to\infty} |f(x_n)| = m.$$

Sur la base de (3), (4) et (5), on conclut que $|f(a)| = m$ et $|a| \leqslant \leqslant r$. □

THÉORÈME 1.5. *Un module de polynôme quelconque f de* $\mathbf{C}[z]$ *atteint sa valeur minimale sur l'ensemble* $\mathbf{C}$.

Démonstration. Le théorème est apparemment vrai si $\deg f = 0$ ou $f(0) = 0$. Supposons donc que $\deg f \geqslant 1$ et $f(0) \neq 0$. Posons $M = |f(0)|$. Selon le théorème 1.1, on a

(1) $$(\exists r > 0)\,(\forall z \in \mathbf{C})\,(|z| \geqslant r \rightarrow |f(z)| \geqslant M).$$

Soit $K = \{z \in \mathbf{C} \,\|\, |z| \leqslant r\}$. Selon le théorème 1.4, $|f|$ admet la plus petite valeur dans le cercle K, c'est-à-dire qu'il existe un nombre a tel que

(2) $$|f(a)| \leqslant |f(z)| \text{ si } |z| \leqslant r, \text{ en particulier,}$$

(3) $$|f(a)| \leqslant |f(0)| = M.$$

Sur la base de (1) et (3), on conclut que

(4) $$|f(a)| \leqslant |f(z)| \text{ si } |z| \geqslant r.$$

En vertu de (2) et (4), il vient $(\forall z \in \mathbf{C})\,(|f(a)| \leqslant |f(z)|)$. Ainsi, $|f|$ atteint sur l'ensemble $\mathbf{C}$ la plus petite valeur au point a. □

Lemme de d'Alembert. La démonstration du théorème 1.7 s'appuie pour une large part sur le lemme suivant dit lemme de d'Alembert.

LEMME 1.6. *Soient $f(x)$ un polynôme de degré positif sur le corps des nombres complexes et $a \in \mathbf{C}$. Si $f(a) \neq 0$, il existe un nombre complexe c tel que $|f(c)| < |f(a)|$.*

Démonstration. Soient $f(x) = a_0 + \ldots + a_n x^n$ un polynôme de degré $n > 0$ et $f(a) \neq 0$. Décomposons f en puissances de la différence $x - a$:

(1) $$f(x) = c_0 + c_1(x-a) + \ldots + c_n(x-a)^n, \text{ où } c_i \in \mathbf{C},$$
$$c_0 = f(a) \neq 0, \quad c_n \neq 0.$$

Posons $z = x - a$ et

(2) $$g(z) = c_0 + c_1 z + \ldots + c_n z^n.$$

Soit c_m un coefficient non nul du polynôme g à un plus petit indice positif $(0 < m \leqslant n)$; alors

(3) $$f(a+z) = g(z) = c_0 + c_m z^m + c_{m+1} z^{m+1} + \ldots + c_n z^n.$$

Définissons $h(z)$:

(4) $$h(z) = \begin{cases} c_{m+1} + \ldots + c_n z^{n-m-1} & \text{si } m < n, \\ 0 \text{ si } m = n. \end{cases}$$

Alors l'égalité (3) peut s'écrire sous forme

(5) $$g(z) = c_0 + c_m z^m + z^{m+1} h(z).$$

En vertu de (1), $\frac{c_0}{c_m} \neq 0$. Notons d une racine m-ième quelconque du nombre $(-c_0/c_m)$:

(6) $$d^m = -c_0/c_m.$$

Considérons dans (5) la valeur de z sous forme

(7) $$z = \lambda d, \text{ où } 0 < \lambda < 1, \quad \lambda \in \mathbf{R}.$$

En vertu de (5) et (6), on obtient les égalités

(8) $$\begin{aligned} g(\lambda d) &= c_0 - c_0 \lambda^m + \lambda^{m+1} d^{m+1} h(\lambda d), \\ g(\lambda d) &= c_0 [1 - \lambda^m + \lambda^{m+1} c_0^{-1} d^{m+1} h(\lambda d)]. \end{aligned}$$

Sur la base de (4), on conclut que

$$d^{m+1} h(\lambda d) = c_{m+1} d^{m+1} + \ldots + c_n d^n \lambda^{n-m-1} \quad (m < n);$$

et

$$|c_0^{-1} d^{m+1} h(\lambda d)| \leqslant |c_0|^{-1} [|c_{m+1} d^{m+1}| + \ldots + |c_n d^n|] \quad (m < n).$$

Posons à présent

(9) $$B = \begin{cases} |c_0|^{-1} [|c_{m+1} d^{m+1}| + \ldots + |c_n d^n|] & \text{si } m < n, \\ 0 \text{ si } m = n. \end{cases}$$

Notons que pour $m < n$, $B > 0$, vu que c_n et d sont différents de zéro.

De (8) et (9) s'ensuit l'inégalité

$$|g(\lambda d)| \leqslant |c_0| [1 - \lambda^m + \lambda^{m+1} B] = |c_0| [1 - \lambda^m (1 - \lambda B)].$$

Si λ satisfait aux conditions $0 < \lambda < 1$, $\lambda B < 1$, $|g(\lambda d)| < |c_0|$. Comme $c_0 = f(a)$ et, en vertu de (3), $g(\lambda d) = f(a + \lambda d)$, on a alors

$$|f(a + \lambda d)| < |f(a)| \text{ si } \begin{cases} 0 < \lambda < \min\{1, B^{-1}\} & \text{pour } m < n, \\ 0 < \lambda < 1 \text{ avec } m = n. \end{cases} \quad \square$$

Fermeture algébrique d'un corps des nombres complexes. Soit $\mathcal{F}[x]$ un anneau des polynômes en x sur le corps $\mathcal{F}$.

DÉFINITION. Un corps $\mathcal{F}$ est dit *algébriquement fermé* si tout polynôme de degré positif de $\mathcal{F}[x]$ possède dans le corps $\mathcal{F}$ une racine au moins.

THÉORÈME 1.7. *Un corps des nombres complexes est algébriquement fermé.*

D é m o n s t r a t i o n. Soit f un polynôme quelconque de degré positif de $F[x]$. Si $f(0) = 0$, alors le zéro est une racine du polynôme f. Admettons que $f(0) \neq 0$ et posons $M = |f(0)|$. Soit r un nombre positif pour lequel

(1) $(\forall z \in \mathbf{C})\,(|z| \geqslant r \to M \leqslant |f(z)|)$.

Ce r existe en vertu du théorème 1.1.

Soit $K = \{z \in \mathbf{C} \mid |z| \leqslant r\}$. En vertu du théorème 1.4, la fonction $|f|$ atteint la plus petite valeur sur l'ensemble K, c'est-à-dire qu'il existe un nombre $a \in K$, tel que

(2) $|f(a)| \leqslant |f(z)|$ pour tout $z \in K\ (|z| \leqslant r)$

et, en particulier,

(3) $|f(a)| \leqslant |f(0)| = M.$

De (1) et (3), il vient

(4) $(\forall z \in \mathbf{C})\,(|z| \geqslant r_0 \to |f(a)| \leqslant |f(z)|)$.

Sur la base de (2) et (4), on conclut que

(5) $(\forall z \in \mathbf{C})\,(|f(a)| \leqslant |f(z)|)$.

Si $f(a) \neq 0$, alors, selon le lemme de d'Alembert, il existe un nombre complexe a tel que

$$|f(c)| < |f(a)| \qquad (c \in \mathbf{C}).$$

Or, cette dernière inégalité est en contradiction avec (5), aussi, le cas de $f(a) \neq 0$ est-il impossible. Par conséquent, $f(a) = 0$, c'est-à-dire le nombre complexe a est une racine du polynôme f. □

COROLLAIRE 1.8. *Tout polynôme de l'anneau $\mathscr{C}[x]$, dont le degré est supérieur à l'unité, est réductible dans l'anneau $\mathscr{C}[x]$.*

D é m o n s t r a t i o n. Soient $f \in \mathscr{C}[x]$ et $\deg f > 1$. Selon le théorème 1.7, il existe un $a \in \mathbf{C}$ tel que $f(a) = 0$. Alors, selon le théorème 14.1.11, $(x - a)$ divise f, c'est-à-dire qu'il existe un polynôme g dans $\mathscr{C}[x]$, tel que $f = (x - a)\cdot g$. En outre, $\deg g > 0$, vu que $\deg f > 1$. Ainsi, le polynôme f est réductible dans l'anneau $\mathscr{C}[x]$.

COROLLAIRE 1.9. *Tout polynôme f de degré positif de l'anneau $\mathscr{C}[x]$ peut être représenté de façon unique sous forme de produit d'un nombre complexe et de facteurs linéaires normés, c'est-à-dire sous forme*

(1) $f = c\,(x - \alpha_1) \ldots (x - \alpha_n)$,

où $\alpha_1, \ldots, \alpha_n$ sont les racines du polynôme f (dans **C**) *et c le coefficient dominant du polynôme.*

Cette affirmation découle du corollaire 1.8 et du théorème 14.2.11 de la décomposition du polynôme sur le corps en un produit de facteurs normés irréductibles.

Si dans la décomposition (1) $\alpha_1, \ldots, \alpha_m$ sont tous les racines distinctes du polynôme f dans C, alors cette décomposition peut être représentée sous forme

$$(2) \quad f = c\,(x - \alpha_1)^{k_1} \ldots (x - \alpha_m)^{k_m}, \; k_1 + \ldots + k_m = n.$$

La décomposition (2) est appelée *décomposition canonique du polynôme f en facteurs irréductibles.* Le nombre k_s est appelé *indice de multiplicité de la racine α_s.*

COROLLAIRE 1.10. *Tout polynôme f de degré positif n de $\mathscr{C}[x]$ admet exactement n racines complexes si l'on compte chaque racine autant de fois que vaut sa multiplicité.*

Formule de Viète. Etablissons la relation entre les racines et les coefficients d'un polynôme.

THÉORÈME 1.11 (DE VIÈTE). *Soient $f = z^n + c_1 z^{n-1} + \ldots + c_{n-1} z + c_n$ un polynôme sur le corps des nombres complexes et $\alpha_1, \ldots, \alpha_n$ ses racines; alors*

$$(1) \quad \begin{aligned} c_1 &= -(\alpha_1 + \alpha_2 + \ldots + \alpha_n); \\ c_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n; \\ c_3 &= -(\alpha_1\alpha_2\alpha_3 + \ldots + \alpha_{n-2}\alpha_{n-1}\alpha_n); \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ c_n &= (-1)^n \alpha_1\alpha_2 \ldots \alpha_n. \end{aligned}$$

D é m o n s t r a t i o n. Vu que $\alpha_1, \ldots, \alpha_n$ sont des racines du polynôme f, selon le corollaire 1.9, il s'ensuit

$$z^n + c_1 z^{n-1} + \ldots + c_{n-1} z + c_n = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_n).$$

En multipliant les facteurs linéaires dans le second membre de l'égalité, on obtient

$$z^n + c_1 z^{n-1} + \ldots + c_{n-1} z + c_n = z^n - (\alpha_1 + \ldots + \alpha_n) z^{n-1} + \ldots + (-1)^n \alpha_1\alpha_2 \ldots \alpha_n.$$

De l'égalité de deux polynômes en z il s'ensuit une égalité des coefficients des mêmes puissances de z; en égalant les coefficients des mêmes puissances de z, on obtient les formules (1). □

Les formules (1) sont appelées *formules de Viète.*

Corollaire 1.12. *Si $\alpha_1, \ldots, \alpha_n$ sont des racines du polynôme $c_0z^n + c_1z^{n-1} + \ldots + c_{n-1}z + c_n$ de degré n de* **C** *[z], alors*

$$\frac{c_1}{c_0} = -(\alpha_1 + \ldots + \alpha_n);$$

$$\frac{c_2}{c_0} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n;$$

. . . .

$$\frac{c_n}{c_0} = (-1)^n \alpha_1\alpha_2 \ldots \alpha_n.$$

Exercices

1. Décomposer en facteurs linéaires dans l'anneau $\mathscr{C}$ [z] les polynômes: (a) $z^2 + z + 1 + i$; (b) $z^4 + z^3 - z - 1$.
2. Décomposer en facteurs irréductibles le polynôme $z^4 + 3z^3 + 4z^2 + 3z + 1$ dans $\mathscr{C}$ [z] et dans $\mathscr{R}$ [z].
3. Décomposer le polynôme $z^n - 1$, où n est un nombre naturel différent de zéro et de 1, en facteurs linéaires dans $\mathscr{C}$ [z].
4. La somme de deux racines de l'équation $2x^3 - x^2 - 7x + \lambda = 0$ est égale à 1. Chercher λ.
5. Déterminer λ de manière que l'une des racines de l'équation $x^3 - 7x + \lambda = 0$ soit égale au double de l'autre.
6. Connaissant que le polynôme $z^n + a_{n-1}z^{n-1} + \ldots + a_1z + a_0$, où $a_{n-1}, \ldots, a_0$ sont des nombres complexes, possède les racines $\alpha_1, \ldots, \alpha_n$, calculer le produit $(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_n + 1)$.
7. Soit $b^2 < 4ac$, où a, b, c sont des nombres réels. Démontrer que l'anneau quotient $\mathscr{R}$ $[z]/(az^2 + bz + c)$ est isomorphe au corps des nombres complexes.
8. Démontrer la proposition inverse du théorème de Viète (théorème 1.11): si l'on a les formules de Viète (formules (1)), alors les nombres complexes $\alpha_1, \ldots, \alpha_n$ sont les racines du polynôme $f = z^n + c_1z^{n-1} + \ldots + c_n$ sur le corps $\mathscr{C}$.

§ 2. Polynômes sur un corps des nombres réels

Conjugaison des racines imaginaires d'un polynôme avec coefficients réels. Soit $\mathscr{R}$ [x] un anneau des polynômes sur un corps $\mathscr{R}$ des nombres réels.

Rappelons qu'un nombre complexe $a + bi$, où $a, b \in$ **R**, est dit imaginaire si $b \neq 0$. Si $\alpha = a + bi$, on notera $\bar{\alpha}$ le nombre complexe conjugué $a - bi$.

Lemme 2.1. *Si f est un polynôme de l'anneau $\mathscr{R}$ [x] et α un nombre complexe quelconque, alors $f(\bar{\alpha}) = \overline{f(\alpha)}$.*

La démonstration découle directement du théorème 4.7.6.

Théorème 2.2. *Soit f un polynôme quelconque de l'anneau $\mathscr{R}$ [x]. Si $a + bi$ est une racine imaginaire du polynôme f, $a - bi$ est également une racine de ce polynôme.*

D é m o n s t r a t i o n. Soit $a + bi$ une racine du polynôme, c'est-à-dire $f(a + bi) = 0$. Alors, selon le lemme 2.1,

$$f(a - bi) = f(\overline{a + bi}) = \overline{f(a + bi)} = \bar{0} = 0,$$

c'est-à-dire $f(a - bi) = 0$. □

Polynômes irréductibles sur le corps des nombres réels.

THÉORÈME 2.3. *Soit f un polynôme dont le degré est supérieur à l'unité, irréductible sur un corps $\mathcal{R}$ des nombres réels. Il existe alors des a, $b \in \mathbf{R}$ tels que $b \neq 0$ et le polynôme f est associé au polynôme $(x-a)^2+b^2$.*

Démonstration. Selon le théorème 1.7, le polynôme f admet au moins une racine complexe. Soit $a+bi$ une racine du polynôme f, où a, $b \in \mathbf{R}$. Si $b=0$, alors $x-a$ divise f, ce qui est en contradiction avec l'hypothèse d'irréductibilité de f sur $\mathcal{R}$. Par conséquent, $b \neq 0$. Appliquons aux polynômes f et $(x-a)^2+b$ le théorème de la division avec reste. Selon ce théorème, il existe dans l'anneau $\mathcal{R}[x]$ des polynômes $q(x)$ et $cx+d$ tels que

$$f(x)=q(x)[(x-a)^2+b^2]+(cx+d), \quad c, d \in \mathbf{R}.$$

En posant dans cette égalité $x=a+bi$, on obtient

$$f(a+bi)=c(a+bi)+d=0, \quad (ca+d)+bci=0.$$

Il s'ensuit que $ca+d=0$, $bc=0$. Or, $b \neq 0$, donc $c=0$ et $d = 0$. Ainsi,

$$f(x)=q(x)[(x-a)^2+b^2].$$

Puisque, par hypothèse, le polynôme f est irréductible sur $\mathcal{R}$, le degré du polynôme $q(x)$ vaut zéro. Par conséquent, le polynôme f est associé au polynôme $(x-a)^2+b^2$. □

COROLLAIRE 2.4. *Dans l'anneau $\mathcal{R}[x]$ ne sont irréductibles que les polynômes du premier degré, ainsi que les polynômes du second degré associés aux polynômes de la forme $(x-a)^2+b^2$, où a et b sont des nombres réels quelconques et $b \neq 0$.*

Du corollaire 2.4 et du théorème 14.2.11 découle le théorème suivant.

THÉORÈME 2.5. *Tout polynôme f de degré positif de l'anneau $\mathcal{R}[x]$ peut être représenté de façon unique sous forme d'un produit d'un nombre réel et de polynômes de 2-ième degré au plus irréductibles sur $\mathcal{R}$:*

$$f=d\prod_k[(x-a_k)^2+b_k^2]\prod_s(x-c_s), \text{ où } b_k \neq 0.$$

COROLLAIRE 2.6. *Tout polynôme à coefficients réels admet un nombre pair de racines imaginaires.*

COROLLAIRE 2.7. *Un polynôme de degré impair à coefficients réels admet au moins une racine réelle.*

COROLLAIRE 2.8. *Soit f un polynôme de degré n de $\mathcal{R}[x]$. La parité du nombre des racines réelles du polynôme f coïncide avec celle du nombre n.*

Exercices

1. Chercher le polynôme aux coefficients réels et de degré minimal admettant les racines $i - 1$, π, $-1 + i\sqrt{3}$.
2. Décomposer en facteurs irréductibles sur le corps des nombres réels les polynômes:

(a) $x^3 + x + 2$; (b) $x^4 + 2x^2 + 4$; (c) $x^6 - 1$; (d) $x^4 - x^2 + 1$.

3. Décomposer le polynôme $x^4 + 4$ en facteurs irréductibles: a) sur le corps $\mathscr{C}$; (b) sur le corps $\mathscr{R}$; (c) sur le corps $\mathfrak{Q}$.
4. Décomposer en facteurs irréductibles sur le corps des nombres réels le polynôme $x^4 - ax^2 + 1$, où $-2 < a < 2$.
5. Démontrer que le polynôme $x^{3m} + x^{3n+1} + x^{3p+2}$ est divisible par le polynôme $x^2 + x + 1$.
6. Soit f un polynôme sur le corps des nombres réels dont le coefficient dominant et le terme libre sont de signes opposés. Démontrer que le polynôme f admet au moins une racine réelle.

§ 3. Equations de troisième et quatrième degrés

Equation de troisième degré. L'équation

(1) $x^3 + px + q = 0 \qquad (p, q \in C)$

est appelée *équation cubique incomplète*. Posons dans l'équation (1) $x = u + v$, c'est-à-dire au lieu d'une variable introduisons deux. On obtient

$$(u + v)^3 + p(u + v) + q = 0,$$

ou

(2) $u^3 + v^3 + q + (3uv + p)(u + v) = 0.$

Exigeons que soit remplie la condition $3uv + p = 0$, autrement dit, la condition $uv = -p/3$. A la satisfaction de cette condition, u et v vérifient le système

(3) $u^3 + v^3 = -q, \qquad uv = -p/3.$

Sur la base de (3), (2) et (1), on conclut: si (u, v) est la solution du système (3) la somme $u + v$ est la solution de l'équation (1).

Montrons que la proposition inverse est également vraie: si x est la racine de l'équation (1), il existe une solution (u, v) du système (3), telle que $x = u + v$. En effet, soit x la racine de l'équation (1). Considérons l'équation

$$y^2 - xy - p/3 = 0.$$

Soient u, v ses racines complexes. Alors, en appliquant les formules de Viète, il vient

$$x = u + v, \qquad uv = -p/3.$$

x étant la racine de l'équation (1), (u, v) est donc la solution de (2) et, partant, la solution du système (3). Ainsi, connaissant la solution du système (3), on peut obtenir toutes les racines de l'équation (1).

Le système d'équations

(4) $\quad u^3 + v^3 = -q, \qquad u^3v^3 = -p^3/27,$

est apparemment impliqué par le système (3). Les nombres u, v satisfont à (4) si et seulement si u^3, v^3 sont des racines de l'équation quadratique

(5) $\quad z^2 + qz - p^3/27 = 0.$

Cette équation est dite *résolvante pour l'équation* (1). Son discriminant est désigné par Δ:

$$\Delta = \frac{q^2}{4} + \frac{p^3}{27}.$$

Les racines z_1, z_2 de l'équation (5) s'expriment par les formules

(6) $\quad z_1 = u^3 = -q/2 + \sqrt{\Delta}, \qquad z_2 = v^3 = -q/2 - \sqrt{\Delta}.$

De là on tire neuf solutions du système (4). En choisissant parmi ces dernières les solutions (u, v) du système (4) qui satisfont à la condition $uv = -p/3$, on obtient toutes les solutions du système (3).

Le système (3) admet une solution au moins. En effet, soit (u_1, v_1) une quelconque des solutions du système (4), alors $u_1^3v_1^3 = -p^3/27$. Par suite,

$$u_1v_1 = -\frac{p}{3}, \text{ ou } u_1v_1 = -\frac{p}{3}\cdot\varepsilon, \text{ ou } u_1v_1 = -\frac{p}{3}\cdot\varepsilon^2, \text{ où } \varepsilon^3 = 1;$$

donc

$$u_1v_1 = -\frac{p}{3}, \text{ ou } u_1(v_1\varepsilon^2) = -\frac{p}{3}, \text{ ou } u_1(v_1\varepsilon) = -\frac{p}{3}.$$

Par conséquent, pour toute valeur u de la racine cubique de z_1 il existe une valeur v de la racine cubique de z_2, telle que $uv = -p/3$, c'est-à-dire que le couple (u, v) sera une solution du système (3).

Si u, $u\varepsilon$, $u\varepsilon^2$ sont les valeurs de la racine cubique de z_1, il leur correspond v, $v\varepsilon^2$, $v\varepsilon$, valeurs de la racine cubique de z_2. Ainsi, si (u, v) est une solution quelconque du système (3), alors (u, v), $(u\varepsilon, v\varepsilon^2)$, $(u\varepsilon^2, v\varepsilon)$ est la collection de toutes les solutions du système (3) qui admet trois solutions différentes. On conclut donc que l'équation (1) admet les solutions suivantes:

(7) $\quad x_1 = u + v, \qquad x_2 = u\varepsilon + v\varepsilon^2, \qquad x_3 = u\varepsilon^2 + v\varepsilon.$

THÉORÈME 3.1. *Soit donnée l'équation*

(1) $\quad x^3 + px + q = 0.$

Soient z_1 *et* z_2 *des racines de l'équation résolvante* $z^2 + qz - p^3/27 = 0.$

Les racines de l'équation (1) *s'expriment par les formules*

(I) $x_1 = u + v, \qquad x_2 = u\varepsilon + v\varepsilon^2, \qquad x_3 = u\varepsilon^2 + v\varepsilon,$

où u et v sont des nombres satisfaisant aux conditions

(*) $u^3 = z_1, \qquad v^3 = z_2, \qquad uv = -p/3,$

et ε est la racine cubique imaginaire de l'unité.

Démonstration. Une vérification directe montre que $x^3 + px + q$ est divisible par $x - x_1$, le quotient étant égal à $x^2 + x_1x + x_1^2 + p$; par conséquent,

(2) $x^3 + px + q = (x - x_1)(x^2 + x_1x + x_1^2 + p).$

Ensuite, on a

(3) $(x - x_2)(x - x_3) = x^2 - (x_2 + x_3)x + x_2x_3.$

En vertu des formules de Viète

(4) $1 + \varepsilon + \varepsilon^2 = 0$ et $\varepsilon + \varepsilon^2 = -1.$

De là et des formules (I), il s'ensuit que

(5) $x_1 + x_2 + x_3 = 0, \qquad -(x_2 + x_3) = x_1.$

En vertu des formules (I), (*) et (4), il vient

$$x_2x_3 = (u\varepsilon + v\varepsilon^2)(u\varepsilon^2 + v\varepsilon) = u^2 + v^2 + uv(\varepsilon^2 + \varepsilon) = \\ = u^2 + v^2 - uv = (u + v)^2 - 3uv = x_1^2 + p,$$

c'est-à-dire

(6) $x_2x_3 = x_1^2 + p.$

En vertu de (5) et (6), la formule (3) peut être écrite sous forme

(7) $(x - x_2)(x - x_3) = x^2 + x_1x + x_1^2 + p.$

En se basant sur (2) et (7), on conclut que

$$x^3 + px + q = (x - x_1)(x - x_2)(x - x_3). \quad \square$$

COROLLAIRE 3.2. *Les racines de l'équation* (1) *s'expriment par les formules*

(II) $x_1 = u + v; \quad x_2 = -\frac{1}{2}(u + v) + i\frac{\sqrt{3}}{2}(u - v);$

$$x_3 = -\frac{1}{2}(u + v) - i\frac{\sqrt{3}}{2}(u - v),$$

où u et v sont des nombres satisfaisant aux conditions (*).

Démonstration. Les formules (II) s'obtiennent à partir des formules (I) si l'on pose $\varepsilon = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$. $\square$

Etude des racines de l'équation de troisième degré avec coefficients réels. Le théorème suivant permet de déterminer le nombre de racines réelles et imaginaires d'une équation du troisième degré.

THÉORÈME 3.3. *Soient*

(1) $x^3 + px + q = 0$

une équation à coefficients réels et $\Delta = \frac{q^2}{4} + \frac{p^3}{27}$. *Alors:*

(a) *si* $\Delta > 0$, *l'équation* (1) *admet une racine réelle et deux imaginaires conjuguées;*

(b) *si* $\Delta = 0$, *les racines de l'équation* (1) *sont réelles et l'une d'elles au moins est multiple;*

(c) *si* $\Delta < 0$, *toutes les racines de l'équation* (1) *sont réelles et distinctes.*

Démonstration. Premier cas: $\Delta > 0$. Dans ce cas les racines z_1 et z_2 de l'équation résolvante sont réelles et distinctes. Par conséquent, l'une d'elles au moins, par exemple, z_1, est différente de zéro. Soit $u = (z_1)^{1/3}$ la racine arithmétique de z_1. Le nombre v est également un nombre réel, vu que $uv = -p/3$. Etant donné que $z_1 \neq z_2$ et, par suite, $u^3 \neq v^3$, on a $u \neq v$. Selon le corollaire 3.2,

$$\text{(II)} \quad x_1 = u + v, \quad x_2 = -\frac{1}{2}(u+v) + i\frac{\sqrt{3}}{2}(u-v),$$

$$x_3 = -\frac{1}{2}(u+v) - i\frac{\sqrt{3}}{2}(u-v).$$

u et v étant des nombres réels distincts, il s'ensuit des formules (II) que x_1 est une racine réelle, tandis que x_2 et x_3 sont des imaginaires conjuguées.

Deuxième cas: $\Delta = 0$. Si $\Delta = 0$ et $q \neq 0$, $z_1 = z_2 = -q/2 \neq 0$. Soit $u = (-q/2)^{1/3}$ une racine arithmétique du nombre $-q/2$. $uv = p/3$ étant un nombre réel, il en résulte que $v = (-q/2)^{1/3}$, c'est-à-dire $u = v \neq 0$. En vertu des formules (II), il s'ensuit:

$$x_1 = 2u \neq 0, \qquad x_2 = x_3 = -u.$$

Ainsi, avec $q \neq 0$ l'équation (I) admet trois racines réelles dont l'une est double.

Mais si $\Delta = 0$ et $q = 0$, alors $p = 0$. Dans ce cas l'équation (1) prend la forme $x^3 = 0$. Par conséquent, $x_1 = x_2 = x_3 = 0$.

Troisième cas: $\Delta < 0$. Dans ce cas $z_1 = -q/2 + \sqrt{\Delta}$, $z_2 = -q/2 - \sqrt{\Delta}$.

Par conséquent, z_1 et z_2 sont des nombres imaginaires conjugués et, partant,

(1) $|z_1| = |z_2| \neq 0$

et

(2) $z_1 \neq z_2$.

En vertu du théorème 3.1, il existe des nombres u et v tels que

(3) $u^3 = z_1, \qquad uv = -p/3, \qquad v^3 = z_2.$

Il s'ensuit de (1) et (3) que $|u|^3 = |v|^3 \neq 0$ et, par suite,

(4) $|u| = |v| \neq 0.$

Ensuite, en vertu de (2),

(5) $u \neq v.$

Sur la base de (3) et (4), on conclut que

(6) $$-\frac{p}{3|u|^2} = 1.$$

Sur la base de (3) et (6), il vient

(7) $$v = -\frac{p}{3u} = -\frac{p}{3u\bar{u}} \cdot \bar{u} = -\frac{p}{3|u|^2} \cdot \bar{u} = \bar{u}.$$

Il s'ensuit de (5) et (7) que u et v sont des nombres imaginaires conjugués. Selon le corollaire 3.2, il vient:

$$x_1 = u + v;$$

(II) $$x_2 = -\frac{1}{2}(u+v) + i\frac{\sqrt{3}}{2}(u-v);$$

$$x_3 = -\frac{1}{2}(u+v) - i\frac{\sqrt{3}}{2}(u-v).$$

Comme $\bar{u} = v$ et $u \neq v$, il s'ensuit de ces formules que toutes les racines x_1, x_2 et x_3 sont réelles. En outre, elles sont deux à deux différentes. En effet, en vertu des formules (II), $x_2 \neq x_3$. Supposons que $x_1 = x_2$. Alors, en vertu des formules (I), $u + v = u\varepsilon + v\varepsilon^2$, d'où $u(1 - \varepsilon) = v(\varepsilon^2 - 1)$; donc, $u = v\varepsilon^2$. De là on tire l'égalité $z_1 = z_2$ et $\Delta = 0$; or cette dernière égalité est en contradiction avec la condition $\Delta < 0$.

De façon analogue on se convainc que $x_1 \neq x_3$. □

Equations de quatrième degré. La méthode de Ferrari permet de résoudre l'équation du quatrième degré en réduisant l'opération à la résolution d'une équation auxiliaire du troisième degré. Le principe de la méthode de Ferrari est le suivant. L'équation donnée du quatrième degré avec coefficients complexes

(1) $x^4 + ax^3 + bx^2 + cx + d = 0$

s'écrit sous forme de $x^4 + ax^3 = -bx^2 - cx - d$. En ajoutant aux deux membres de l'équation $a^2x^2/4$, il vient

$$\left(x^2 + \frac{ax}{2}\right)^2 = \left(\frac{a^2}{4} - b\right)x^2 - cx - d.$$

Ensuite, en additionnant aux deux membres de l'équation la somme

$$\left(x^2+\frac{ax}{2}\right)y+\frac{y^2}{4},$$

on obtient dans le premier membre de l'équation un carré parfait:

$$(2)\qquad \left(x^2+\frac{ax}{2}+\frac{y}{2}\right)^2=\left(\frac{a^2}{4}-b+y\right)x^2+\left(\frac{ay}{2}-c\right)x+\frac{y^2}{4}-d.$$

Le trinôme à droite est fonction du paramètre y. Choisissons ce paramètre y de manière que le trinôme soit un carré d'un binôme du premier degré en x. Pour que le trinôme $Ax^2 + Bx + C$ soit un carré du binôme en x, il suffit que $B^2 - 4AC = 0$. De fait, en remplissant cette condition, il vient

$$Ax^2+Bx+C=Ax^2+2\sqrt{AC}\,x+C=(\sqrt{A}x+\sqrt{C})^2.$$

Il faut donc choisir y dans le second membre de (2) de manière que soit remplie la condition

$$\left(\frac{ay}{2}-c\right)^2-4\left(\frac{a^2}{4}-b+y\right)\left(\frac{y^2}{4}-d\right)=0,$$

qu'on peut écrire sous forme

$$(3)\qquad y^3-by^2+(ac-4d)\,y-[c^2+d\,(a^2-4b)]=0.$$

Cette condition étant remplie, le second membre de l'équation (2) sera un carré d'un binôme linéaire en x.

En résolvant l'équation auxiliaire (3), on obtient l'une de ses racines y_0. Ensuite, cherchons les nombres m et n rendant le carré du binôme $mx + n$ égal au second membre de l'égalité (2), alors

$$(4)\qquad \left(x^2+\frac{ax}{2}+\frac{y_0}{2}\right)^2=(mx+n)^2,$$

où $m=\sqrt{\frac{a^2}{4}-b+y_0}$, $n=\sqrt{\frac{y_0^2}{4}-d}$. La résolution de l'équation (4) se réduit à la résolution du système de deux équations quadratiques suivantes:

$$x^2+\frac{ax}{2}+\frac{y_0}{2}=mx+n,\qquad x^2+\frac{ax}{2}+\frac{y_0}{2}=-mx-n.$$

Ces deux équations une fois résolues, on obtient quatre racines de l'équation de départ (1).

Exercices

1. Résoudre les équations suivantes du troisième degré:

(a) $x^3 - 3x + 2 = 0$; (b) $x^3 - 6x + 4 = 0$;
(c) $x^3 + 3x - x + 4 = 0$; (d) $x^3 + 3x - 2i = 0$.

2. Résoudre les équations du quatrième degré suivantes:

(a) $x^4 + 2x^3 + 2x^2 + x - 7 = 0$;

(b) $x^4 - x^3 - x^2 + 2x - 2 = 0$;
(c) $x^4 + 12x + 3 = 0$.

3. Démontrer que $(x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 = -4p^3 - 27q^2$, où x_1, x_2, x_3 sont les racines de l'équation $x^3 + px + q = 0$.

§ 4. Séparation des racines réelles d'un polynôme

Système des polynômes de Sturm. Soit f un polynôme à coefficients réels, a et b, $a < b$ étant des nombres réels quelconques ne constituant pas des racines du polynôme.

Plus bas, en recourant à la méthode de Sturm, on résout le problème consistant à trouver le nombre exact des racines réelles distinctes du polynôme f dans l'intervalle $a < x < b$.

Supposons donnée la suite finie des nombres réels, par exemple, 2, 5, —3, 4, —5, —2, 7. Les signes des nombres de cette suite alternent de la façon suivante: +, +, —, +, —, —, + et varient quatre fois. Ainsi, dans cette suite on a quatre variations de signes.

Soit f un polynôme de degré positif avec coefficients réels et démuni de racines réelles multiples. Définissons la suite finie des polynômes $f_0, f_1, f_2, \ldots, f_m$ sur la base d'un polynôme donné $f_0 = f$, de la façon suivante:

$$f_1 = f', \text{ où } f' \text{ est la dérivée de } f;$$
$$f_0 = q_1 f_1 - f_2;$$
$$f_1 = q_2 f_2 - f_3;$$
$$\cdots\cdots\cdots$$
$$f_{m-1} = q_m f_m.$$

On a ainsi appliqué aux polynômes f et f' l'algorithme d'Euclide) (méthode de divisions successives) en attribuant à chaque variation du reste un signe opposé.

DÉFINITION. La suite des polynômes $f_0, f_1, f_2, \ldots, f_m$ est appelée *système des polynômes f de Sturm.*

Notons quelques propriétés des polynômes du système de Sturm.

PROPRIÉTÉ 4.1. *Tous deux polynômes voisins du système de Sturm sont démunis de racines réelles communes.*

D é m o n s t r a t i o n. Cette affirmation est vraie pour les polynômes f_0 et f_1 ($f_0 = f$, $f_1 = f'$), vu que f n'a pas de racines réelles multiples. Trois polynômes qui se suivent sont liés par l'égalité

$$(*) \quad f_{k-1} = q_k f_k - f_{k+1}.$$

En vertu de cette égalité l'annulation simultanée des deux polynômes voisins f_k et f_{k+1} entraînerait l'annulation simultanée de f_{k-1} et f_k, ensuite, des polynômes f_{k-2} et f_{k-1}, etc., et enfin des polynômes f_0 et f_1, ce qui est impossible. □

PROPRIÉTÉ 4.2. *Si γ est une racine réelle d'un polynôme intermédiaire f_k, $1 \leqslant k < m$, alors les nombres $f_{k-1}(\gamma)$ et $f_{k+1}(\gamma)$ sont de signes différents.*

Démonstration. En effet, si $f_k(\gamma) = 0$, alors en posant dans l'égalité (*) $x = \gamma$, il vient $f_{k-1}(\gamma) = -f_{k+1}(\gamma)$. □

Théorème de Sturm. Pour démontrer le théorème de Sturm on utilisera le théorème suivant de Weierstrass: si une fonction réelle f est continue sur l'intervalle $[a, b]$ et les nombres $f(a)$, $f(b)$ sont de signes opposés, alors f admet une racine entre a et b.

Soit f un polynôme aux coefficients réels. Supposons que pour chaque nombre réel c, $w(c)$ désigne le nombre de variations de signe dans la série numérique $f_0(c), f_1(c), \ldots, f_m(c)$ dans laquelle on a omis tous les zéros.

THÉORÈME (DE STURM). *Soient f un polynôme à coefficients réels ne possédant pas de racines réelles multiples et*

(1) $f_0, f_1, \ldots, f_m$

le système des polynômes f de Sturm. Soient a et b $(a < b)$ des nombres réels quelconques qui ne sont pas des racines du polynôme f. Le nombre des racines réelles distinctes du polynôme f dans l'intervalle (a, b) est égal à la différence $w(a) - w(b)$.

Démonstration. Soit M l'ensemble de toutes les racines réelles des polynômes (1). Les éléments de l'ensemble M divisent l'intervalle (a, b) en sous-intervalles. Dans chacun de ces sous-intervalles aucun des polynômes (1) ne s'annule. En vertu du théorème de Weierstrass, il s'ensuit que dans chacun des sous-intervalles tous les polynômes (1) conservent leur signe et, partant, le nombre $w(c)$ ne varie pas. Il nous reste à déceler comment varie le nombre $w(c)$ en passant par la valeur réelle γ pour laquelle s'annule un au moins des polynômes (1), c'est-à-dire $\gamma \in M$.

Soient α et β $(\alpha < \beta)$ des points intérieurs de deux sous-intervalles voisins adjacents au point γ. Démontrons que la différence $w(\alpha) - w(\beta)$ s'exprime par les formules

$$(2) \quad w(\alpha) - w(\beta) = \begin{cases} 1 \text{ si } f(\gamma) = 0, \\ 0 \text{ si } f(\gamma) \neq 0. \end{cases}$$

Admettons que γ est la racine du polynôme f_k, où $1 \leqslant k < m$. Selon la propriété 4.2, les nombres $f_{k-1}(\gamma)$ et $f_{k+1}(\gamma)$ possèdent des signes opposés. Donc, dans deux sous-intervalles adjacents à γ les valeurs des polynômes f_{k-1} et f_{k+1} sont affectées de signes opposés. Par conséquent, le nombre de variations des signes dans les suites

$$f_{k-1}(\alpha),\ f_k(\alpha),\ f_{k+1}(\alpha) \text{ et } f_{k-1}(\beta),\ f_k(\beta),\ f_{k+1}(\beta)$$

est le même, à savoir est égal à l'unité. Dans les autres parties du système des polynômes (1) le nombre de variations des signes reste inchangé. Par conséquent, dans le cas considéré $w(\alpha) - w(\beta) = 0$.

Supposons maintenant que γ est la racine du polynôme f ($f = f_0$, $f_1 = f'$). Etant donné que, par hypothèse, le polynôme f est démuni de racines réelles multiples, il existe un polynôme g à coefficients réels, tels que

(3) $$f_0(x) = (x - \gamma)\, g(x), \quad g(\gamma) \neq 0;$$

par conséquent,

(4) $$f_1(x) = g(x) + (x - \gamma)\, g'(x).$$

En vertu de (4) le signe du polynôme f_1 au point γ et, par suite, dans les deux sous-intervalles adjacents à γ coïncide avec celui du nombre $g(\gamma)$. Or, en vertu de (3), le signe de f_0 pour chaque valeur de x coïncide avec celui de $(x - \gamma)\, g(\gamma)$. Donc, entre $f_0(\alpha)$ et $f_1(\alpha)$ on n'a qu'une variation de signe, quant aux nombres $f_0(\beta)$ et $f_1(\beta)$, ils sont affectés du même signe. En outre, toutes les autres variations possibles de signe dans la série (1), comme on l'a déjà montré, se maintiennent avec le passage par le point γ. Ainsi, dans le cas considéré on a $w(\alpha) - w(\beta) = 1$.

Bref, on a démontré que c'est seulement avec le passage par la valeur de la racine du polynôme f que le nombre $w(c)$ diminue d'une unité. Par conséquent, le nombre de racines réelles distinctes du polynôme f est égal à la différence $w(a) - w(b)$. □

Le théorème de Sturm se vérifie également dans le cas où le polynôme admet des racines réelles multiples. La démonstration du théorème dans ce cas diffère peu de celle donnée plus haut.

Pour déterminer le nombre de toutes les racines réelles distinctes du polynôme f en se servant du théorème de Sturm, il faut choisir a et b de manière qu'aucun des polynômes du système de Sturm n'admette des racines à l'extérieur de l'intervalle $a \leqslant x \leqslant b$. Dans ce cas les signes des polynômes du système de Sturm se détermineront par leurs coefficients dominants. En effet, pour de très grandes valeurs de x le signe du polynôme $a_0x^n + a_1x^{n-1} + \ldots + a_n$ coïncide avec celui de a_0, tandis que pour de très grandes valeurs absolues des valeurs négatives de x le signe du polynôme coïncide avec celui de $(-1)^n a_0$. Il n'est donc pas nécessaire de garantir des valeurs suffisamment grandes à a et b, car il suffit de connaître les signes des coefficients dominants des polynômes f du système de Sturm, ainsi que les degrés de ces polynômes.

En utilisant le théorème de Sturm, on peut séparer les racines réelles du polynôme f et, par suite, trouver les intervalles ne contenant chacun qu'une racine du polynôme f.

E x e m p l e. Cherchons le nombre des racines positives et négatives du polynôme $f = x^4 - 4x^2 + x + 1$.

En appliquant la méthode des divisions successives, on trouve pour f le système suivant des polynômes de Sturm :

$$f_0 = f = x^4 - 4x^2 + x + 1;$$
$$f_1 = 4x^3 - 8x + 1;$$
$$f_2 = 8x^2 - 3x - 4;$$
$$f_3 = 87x - 28;$$
$$f_4 = 1.$$

Pour une valeur négative et suffisamment grande en valeur absolue de x la série des signes sera $+, -, +, -, +$ (quatre variations de signe). Pour $x = 0$ les signes coïncident avec ceux des termes libres, c'est-à-dire $+, +, -, -, +$ (deux variations de signe).

Ainsi, on a perdu deux variations de signe, donc le polynôme f admet deux racines négatives. Pour une valeur positive suffisamment grande de x les signes des termes dominants sont $+, +, +, +, +$ (zéro variations de signe). Par conséquent, le polynôme admet deux racines positives.

Exercices

1. Composer les polynômes de Sturm et séparer les racines des polynômes: (a) $x^3 - 3x - 3$; (b) $x^4 - x - 1$; (c) $x^4 - 4x^3 + 4x^2 - 4$; (d) $x^4 - 4x^2 - 1$.

2. Déterminer à l'aide du théorème de Sturm le nombre des racines réelles du polynôme $x^5 + px + q$ avec coefficients réels p et q.

3. Déterminer à l'aide du théorème de Sturm le nombre des racines réelles du polynôme $x^n + px + q$ avec p et q réels.

4. Démontrer que si le système de Sturm pour le polynôme f de degré n avec coefficients réels est composé de $n + 1$ polynômes, alors le nombre de variations de signe dans la série des coefficients dominants des polynômes de Sturm est égal au nombre de couples de racines complexes conjuguées du polynôme f.

5. Chercher le nombre des racines réelles du polynôme $x^4 - 2x^2 + 4x - 1$. Entre quels entiers successifs se disposent ces racines?

CHAPITRE XVII

POLYNÔMES SUR UN CORPS DES NOMBRES RATIONNELS ET NOMBRES ALGÉBRIQUES

§ 1. Racines entières et rationnelles d'un polynôme. Critère d'irréductibilité

Racines entières et rationnelles d'un polynôme. Le théorème suivant nous permet de trouver les racines rationnelles d'un polynôme à coefficients entiers.

THÉORÈME 1.1. *Soient m et q des entiers premiers entre eux et $q \neq 0$. Si m/q est une racine du polynôme $a_0 + a_1x + \ldots + a_nx^n$ à coefficients entiers, alors m divise a_0 et q divise a_n.*

Démonstration. Par hypothèse,

$$a_0 + a_1 \frac{m}{q} + \ldots + a_{n-1} \left(\frac{m}{q}\right)^{n-1} + a_n \left(\frac{m}{q}\right)^n = 0.$$

En multipliant les deux membres de l'égalité par q^n, on obtient

$$(1) \quad a_0q^n + a_1mq^{n-1} + \ldots + a_{n-1}m^{n-1}q + a_nm^n = 0.$$

Sur la base de l'égalité (1) on conclut que m divise a_0q^n. Or, comme les nombres m et q sont premiers entre eux, les nombres m et q^n le sont aussi. Donc, m divise a_0.

En vertu de (1), q divise a_nm^n. En outre, les nombres q et m^n sont premiers entre eux car par hypothèse, les nombres q et m sont premiers entre eux. Par conséquent, q divise a_n. □

COROLLAIRE 1.2. *Si un entier m est une racine du polynôme $a_0 + a_1x + \ldots + a_nx^n$ à coefficients entiers, alors m divise le terme libre a_0.*

COROLLAIRE 1.3. *Une racine rationnelle d'un polynôme ordonné $a_0 + a_1x + \ldots + x^n$ à coefficients entiers est un nombre entier.*

Critère d'irréductibilité d'Eisenstein. Le problème de réductibilité d'un polynôme dans l'anneau $\mathfrak{Q}[x]$ se réduit à celui de réductibilité dans l'anneau $\mathfrak{Z}[x]$.

PROPOSITION 1.4. *Soit f un polynôme de l'anneau des polynômes $\mathfrak{Z}[x]$. Si le polynôme f est réductible dans l'anneau $\mathfrak{Q}[x]$ il est alors réductible dans l'anneau $\mathfrak{Z}[x]$.*

Puisque le corps $\mathfrak{Q}$ est un corps des quotients de l'anneau $\mathfrak{Z}$ des entiers, la proposition 1.4 découle directement du lemme 14.3.5.

THÉORÈME 1.5. (CRITÈRE D'EISENSTEIN). *Soit $f = c_0 + c_1x + \ldots + c_nx^n$ un polynôme avec coefficients entiers. Supposons que tous*

les coefficients du polynôme f excepté le coefficient dominant se divisent par un nombre premier p quelconque, tandis que le terme libre c_0 *n'est pas divisible par* p^2. *Alors le polynôme f est irréductible dans l'anneau* $\mathcal{Q}[x]$.

D é m o n s t r a t i o n. Supposons que le polynôme f est réductible dans l'anneau $\mathcal{Q}[x]$. Alors, en vertu de la proposition 1.4, il est réductible dans l'anneau $\mathbf{Z}[x]$, c'est-à-dire il existe dans $\mathbf{Z}[x]$ des polynômes g et h de degré positif tels que $f = gh$. Soit

$$g = a_0 + \ldots + a_k x^k, \quad h = b_0 + \ldots + b_m x^m \qquad (a_k \neq 0, \quad b_m \neq 0);$$

alors

$$(1) \quad f = (a_0 + \ldots + a_k x^k)(b_0 + \ldots + b_m x^m) = c_0 + c_1 x + \ldots + c_n x^n,$$

avec $1 \leqslant k, m < n$,

$$(2) \quad c_0 = a_0 b_0,$$

$$(3) \quad c_n = a_k b_m.$$

Par hypothèse,

$$(4) \quad p \mid c_0, \quad p^2 \nmid c_0.$$

En vertu de (2) et (4), un seul des nombres a_0 et b_0 est divisible par p ; soit

$$(5) \quad p \mid a_0, \quad p \nmid b_0.$$

Par hypothèse, $p \nmid c_n$. De là, en vertu de (3), il s'ensuit que

$$(6) \quad p \nmid a_k.$$

Supposons que a_s qui n'est pas divisible par p est un coefficient du polynôme g dont l'indice est le plus petit, c'est-à-dire

$$(7) \quad p \mid a_0, \ldots, p \mid a_{s-1}, \qquad p \nmid a_s \qquad (1 \leqslant s \leqslant k < n).$$

En vertu de (1), le coefficient c_s peut être représenté sous forme

$$c_s = a_s b_0 + (a_{s-1} b_1 + \ldots + a_0 b_s) \qquad (s < n).$$

Il s'ensuit de (7) que p divise $a_{s-1} b_1 + \ldots + a_0 b_s$, et comme p ne divise pas b_0 et a_s, p ne divise pas c_s, avec $s \leqslant k < n$. C'est en contradiction avec l'hypothèse du théorème puisque d'après cette dernière, p divise les coefficients $c_0, c_1, \ldots, c_{n-1}$. □

COROLLAIRE 1.6. *Si p est premier et n est un entier positif quelconque, alors le polynôme* $x^n - p$ *est irréductible dans l'anneau* $\mathcal{Q}[x]$.

Exercices

1. Démontrer que le polynôme f à coefficients entiers n'admet pas de racines entières si $f(0)$ et $f(1)$ sont des nombres impairs.

2. Etablir lesquels des polynômes suivants sont irréductibles sur le corps des nombres rationnels:

(a) $2x^5 + 6x^4 - 9x^2 + 12$; (b) $x^2 + x + 1$;

(c) $x^2 + 3x - 4$; (d) $x^3 - 12$; (e) $x^3 + x - 2$;

(f) $x^3 - 3x + 5$; (g) $x^4 - 2x + 3$.

3. Démontrer que le polynôme $\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$, où p est premier, est irréductible sur le corps des nombres rationnels.

4. Démontrer que le polynôme $x^3 - p$, où p est premier, est irréductible sur le corps des nombres rationnels.

5. Pour quels entiers n le polynôme $x^3 + n$ est réductible sur le corps des nombres rationnels?

6. Pour quels entiers m et n le polynôme $mx^3 + n$ est réductible sur le corps des nombres rationnels?

7. Décomposer les polynômes $x^6 - 1$ et $x^8 - 1$ en facteurs irréductibles sur le corps des nombres rationnels.

8. Trouver les conditions de réductibilité du polynôme $x^4 + \alpha x^2 + \beta$, où α, β sont des nombres rationnels, sur le corps des nombres rationnels.

9. Démontrer que si le polynôme f est irréductible sur le corps $\mathcal{Q}$ des nombres rationnels, alors le polynôme $f(\alpha x + \beta)$, où α, β sont des nombres rationnels et $\alpha \neq 0$, est également irréductible sur le corps $\mathcal{Q}$.

§ 2. Extension algébrique simple d'un corps

Extension simple d'un corps. Soit $\mathcal{P}[x]$ un anneau des polynômes en x sur le corps $\mathcal{P}$, où $\mathcal{P}$ est un sous-corps du corps $\mathcal{F}$. Rappelons que l'élément α du corps $\mathcal{F}$ est appelé *algébrique sur le corps* $\mathcal{P}$ si α est une racine d'un polynôme quelconque de degré positif de $\mathcal{P}[x]$.

DÉFINITION. Soient $\mathcal{P} \sqsubseteq \mathcal{F}$ et $\alpha \in F$. On appelle *extension simple du corps* $\mathcal{P}$ *par adjonction de l'élément* α le plus petit sous-corps du corps $\mathcal{F}$ contenant l'ensemble P et l'élément α. L'extension simple $\mathcal{P}$ par adjonction de α est notée $\mathcal{P}(\alpha)$, quant à l'ensemble de base du corps $\mathcal{P}(\alpha)$, il est noté $P(\alpha)$.

Soient $\alpha \in F$, $\mathcal{P}[x]$ un anneau des polynômes en x et

$$P[\alpha] = \{f(\alpha) \mid f \in P[x]\},$$

c'est-à-dire $P[\alpha]$ est un ensemble de toutes les expressions de la forme $a_0 + a_1\alpha + \ldots + a_n\alpha^n$, où $a_0, a_1, \ldots, a_n \in P$ et n un nombre naturel quelconque.

On voit sans peine que l'algèbre $\langle P[\alpha], +, -, \cdot, 1\rangle$, sous-anneau du corps $\mathcal{P}(\alpha)$, est un anneau; cet anneau est désigné par le symbole $\mathcal{P}[\alpha]$.

THÉORÈME 2.1. *Soient $\mathcal{P}[x]$ un anneau des polynômes en x sur $\mathcal{P}$ et $\mathcal{P}(\alpha)$ une extension simple du corps $\mathcal{P}$. Soit ψ une application de*

$P[x]$ sur $P[\alpha]$ telle que $\psi(f) = f(\alpha)$ pour tout f de $P[x]$. Alors:

(a) *pour tout a de P $\psi(a) = a$;*
(b) $\psi(x) = \alpha$;
(c) *ψ est un homomorphisme de l'anneau $\mathcal{P}[x]$ sur l'anneau $\mathcal{P}[\alpha]$;*
(d) $\operatorname{Ker}\psi = \{f \in P[x] \mid f(\alpha) = 0\}$;
(e) *l'anneau quotient $\mathcal{P}[x]/\operatorname{Ker}\psi$ est isomorphe à l'anneau $\mathcal{P}[\alpha]$.*

Démonstration. Les affirmations (a) et (b) s'ensuivent directement de la définition de ψ. L'application ψ respecte les opérations principales de l'anneau $\mathcal{P}[x]$, car pour tous f et g de $P[x]$, on a

$$\psi(f+g) = f(\alpha) + g(\alpha), \quad \psi(fg) = f(\alpha)\,g(\alpha), \quad \psi(1) = 1.$$

Ensuite, par hypothèse, ψ est une application de $P[x]$ sur $P[\alpha]$. Par conséquent, ψ est un homomorphisme de l'anneau $\mathcal{P}[x]$ sur l'anneau $\mathcal{P}[\alpha]$.

L'affirmation (d) découle directement de la définition de l'application ψ.

Puisque ψ est un homomorphisme de l'anneau $\mathcal{P}[x]$ sur $\mathcal{P}[\alpha]$, selon le théorème 13.1.6, l'anneau quotient $\mathcal{P}[x]/\operatorname{Ker}\psi$ est isomorphe à l'anneau $\mathcal{P}[\alpha]$. □

COROLLAIRE 2.2. *Soit α un élément transcendant sur le corps $\mathcal{P}$. Alors l'anneau des polynômes $\mathcal{P}[x]$ est isomorphe à l'anneau $\mathcal{P}[\alpha]$.*

Démonstration. En vertu de la transcendance de α sur $\mathcal{P}$, $\operatorname{Ker}\psi = \{0\}$. Donc, selon le théorème 13.1.6, $\mathcal{P}[x]/\{0\} \cong \cong \mathcal{P}[\alpha]$. En outre, l'anneau quotient de l'anneau $\mathcal{P}[x]$ suivant l'idéal zéro est isomorphe à $\mathcal{P}[x]$. Par conséquent, $\mathcal{P}[x] \cong \cong \mathcal{P}[\alpha]$. □

Polynôme minimal de l'élément algébrique. Soit $\mathcal{P}[x]$ un anneau des polynômes sur le corps $\mathcal{P}$.

DÉFINITION. Soit α un élément algébrique sur le corps $\mathcal{P}$. On appelle *polynôme minimal de l'élément α sur $\mathcal{P}$* le polynôme normé de $\mathcal{P}[x]$ de degré minimal admettant pour racine α. Le degré du polynôme minimal est appelé *degré de l'élément α sur $\mathcal{P}$.*

On voit aisément que pour tout élément α algébrique sur $\mathcal{P}$ il existe un polynôme minimal.

PROPOSITION 2.3. *Si α est un élément algébrique sur le corps $\mathcal{P}$ et g et φ ses polynômes minimaux sur $\mathcal{P}$, alors $g = \varphi$.*

Démonstration. Les degrés des polynômes minimaux g et φ coïncident. Si $g \neq \varphi$, l'élément α (de degré n sur $\mathcal{P}$) est la racine du polynôme $g - \varphi$, dont le degré est inférieur à celui du polynôme φ (inférieur à n), ce qui est impossible. Par conséquent, $g = = \varphi$. □

THÉORÈME 2.4. *Soient α un élément algébrique de degré n sur le corps $\mathcal{P}$ ($\alpha \notin P$) et g son polynôme minimal sur $\mathcal{P}$. Alors:*

(a) *le polynôme g est irréductible dans l'anneau $\mathcal{P}[x]$;*
(b) *si $f(\alpha) = 0$, où $f \in P[x]$, alors g divise f;*
(c) *l'anneau quotient $\mathcal{P}[x]/(g)$ est isomorphe à l'anneau $\mathcal{P}[\alpha]$;*
(d) *$\mathcal{P}[x]/(g)$ est un corps;*
(e) *l'anneau $\mathcal{P}[\alpha]$ coïncide avec le corps $\mathcal{P}(\alpha)$.*

D é m o n s t r a t i o n. Supposons que le polynôme g est réductible dans l'anneau $\mathcal{P}[x]$, c'est-à-dire il existe dans $P[x]$ des dolynômes φ et h tels que

$$g = \varphi h, \qquad 1 \leqslant \deg \varphi, \qquad \deg h < \deg g = n.$$

Dans ce cas $g(\alpha) = \varphi(\alpha) h(\alpha) = 0$. $\mathcal{P}(\alpha)$ étant un corps, $\varphi(\alpha) = 0$ ou $h(\alpha) = 0$, ce qui est impossible, vu que par hypothèse, le degré de l'élément α sur $\mathcal{P}$ vaut n.

Supposons que $f \in P[x]$ et $f(\alpha) = 0$. Par hypothèse $g(\alpha) = 0$. Donc, f et g ne peuvent être premiers entre eux. Le polynôme g étant irréductible, il divise, par conséquent, f.

Soit ψ un homomorphisme de l'anneau $\mathcal{P}[x]$ sur l'anneau $\mathcal{P}[\alpha]$ ($\psi(f) = f(\alpha)$ pour tout f de $P[x]$), considéré dans le théorème 2.1. En vertu de (b), le noyau de l'homomorphisme ψ est composé des polynômes multiples de g, c'est-à-dire $\operatorname{Ker} \psi = (g)$. Par conséquent, selon le théorème 13.1.6, l'anneau quotient $\overline{\mathcal{P}} = \mathcal{P}[x]/(g)$ est isomorphe à l'anneau $\mathcal{P}[\alpha]$.

Puisque $P[\alpha] \subset P(\alpha)$, $\mathcal{P}[\alpha]$ est un domaine d'intégrité. Comme $\overline{\mathcal{P}} \cong \mathcal{P}[\alpha]$, l'anneau quotient $\overline{\mathcal{P}}$ est également un domaine d'intégrité. Il nous faut montrer que tout élément $\overline{f}$ non nul de $\overline{\mathcal{P}}$ est inversible dans $\overline{\mathcal{P}}$. Soit f un élément de la classe suivant un sous-groupe $\overline{f}$. Comme $\overline{f} \neq \overline{0}$, $f(\alpha) \neq 0$ également; donc, le polynôme g ne divise pas le polynôme f. Le polynôme g étant irréductible, il s'ensuit que les polynômes f et g sont premiers entre eux. Par conséquent, il existe dans $P[x]$ des polynômes u et v tels que $uf + vg = 1$. Il s'ensuit l'égalité $\overline{u}\overline{f} = \overline{1}$ montrant que l'élément $\overline{f}$ est inversible dans l'anneau $\overline{\mathcal{P}}$. Bref, on a établi que l'anneau quotient $\overline{\mathcal{P}}$ est un corps.

En vertu de (c) et (d) $\mathcal{P}[\alpha]$ est un corps et, par suite, $P(\alpha) \subset P[\alpha]$. En outre, il est évident que $P[\alpha] \subset P(\alpha)$. Par suite, $P[\alpha] = P(\alpha)$. Par conséquent, l'anneau $\mathcal{P}[\alpha]$ coïncide avec le corps $\mathcal{P}(\alpha)$. □

Structure de l'extension algébrique simple d'un corps.

THÉORÈME 2.5. *Soit α un élément algébrique de degré positif n sur le corps $\mathcal{P}$. Alors tout élément du corps $\mathcal{P}(\alpha)$ peut être représenté de façon unique sous forme de combinaison linéaire de n éléments* $1, \alpha, \ldots, \alpha^{n-1}$ *avec coefficients dans P.*

D é m o n s t r a t i o n. Soit β un élément quelconque du corps $\mathcal{P}(\alpha)$. Selon le théorème 2.4, $P(\alpha) = P[\alpha]$; il existe donc dans $P[x]$ un polynôme f tel que

(1) $\beta = f(\alpha)$.

Soit g un polynôme minimal pour α sur $\mathcal{P}$; en vertu des conditions du théorème, son degré vaut n. Selon le théorème de la division avec reste, il existe dans $P[x]$ des polynômes h et r tels que

(2) $f = gh + r$, où $r = 0$ ou $\deg r < \deg g = n$, c'est-à-dire

$$r = c_0 + c_1x + \ldots + c_{n-1}x^{n-1} \quad (c_i \in P).$$

En posant dans (2) $x = \alpha$ et, compte tenu de l'égalité (1), il vient

(3) $\beta = c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}$.

Montrons que l'élément β est représentable de façon unique sous forme d'une combinaison linéaire d'éléments $1, \alpha, \ldots, \alpha^{n-1}$. Soit

(4) $\beta = d_0 + d_1\alpha + \ldots + d_{n-1}\alpha^{n-1} \qquad (d_i \in P)$

une quelconque de ces représentations. Considérons le polynôme φ

$$\varphi = (c_0 - d_0) + (c_1 - d_1)x + \ldots + (c_{n-1} - d_{n-1})x^{n-1}.$$

Le cas où le degré de φ est inférieur à n est impossible, car en vertu de (3) et (4), $\varphi(\alpha) = 0$ et le degré de φ est inférieur à celui de g. Seul est possible le cas où $\varphi = 0$, c'est-à-dire $c_0 = d_0, \ldots, c_{n-1} = d_{n-1}$. Par conséquent, l'élément β est représentable de façon unique sous forme d'une combinaison linéaire d'éléments $1, \alpha, \ldots, \alpha^{n-1}$. □

Levée de l'irrationalité algébrique dans le dénominateur d'une fraction. Le problème de la levée de l'irrationalité algébrique dans le dénominateur d'une fraction est le suivant. Soit α un élément algébrique de degré $n > 1$ sur le corps $\mathcal{P}$; f et h sont des polynômes de l'anneau des polynômes $\mathcal{P}[x]$ et $h(\alpha) \neq 0$. Il s'agit de représenter l'élément $\frac{f(\alpha)}{h(\alpha)} \in P(\alpha)$ sous forme d'une combinaison linéaire de puissances de l'élément α, c'est-à-dire sous forme de $\varphi(\alpha)$, où $\varphi \in P[x]$.

Ce problème se résout de la façon suivante. Soit g le polynôme minimal pour α sur $\mathcal{P}$. Vu que, selon le théorème 2.4, le polynôme est irréductible sur $\mathcal{P}$ et $h(\alpha) \neq 0$, g ne divise pas h et, par suite, les polynômes h et g sont premiers entre eux. Il existe donc dans $P[x]$ des polynômes u et v tels que

(1) $uh + vg = 1$.

Puisque $g(\alpha) = 0$, de (1) il s'ensuit que

$$u(\alpha)h(\alpha) = 1, \qquad \frac{1}{h(\alpha)} = u(\alpha).$$

Par conséquent, $f(\alpha)/h(\alpha) = f(\alpha)\,u(\alpha)$, avec $f, u \in P[x]$ et $f(\alpha)\,u(\alpha) \in P[\alpha]$. Bref, on s'est libéré de l'irrationalité dans le dénominateur de la fraction $\frac{f(\alpha)}{h(\alpha)}$.

Exercices

1. Chercher le polynôme minimal pour α sur le corps $\mathscr{P}$ si :

(a) $\alpha = -i$, $\mathscr{P} = \mathscr{R}$; (b) $\alpha = i\sqrt{2}$, $\mathscr{P} = \mathscr{C}$;

(c) $\alpha = i\sqrt{2}$; $\mathscr{P} = \mathscr{Q}$; d) $\alpha = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $\mathscr{P} = \mathscr{Q}$;

(e) $\alpha = \sqrt[4]{2}$, $\mathscr{P} = \mathscr{Q}$.

2. Lever l'irrationalité algébrique dans le dénominateur de la fraction $\frac{1}{\sqrt[3]{4} - 2\sqrt[3]{2} - 1}$.

3. Lever l'irrationalité dans le dénominateur de la fraction $\frac{1}{\sqrt{2} + 2\sqrt[4]{2} - 1}$.

§ 3. Extension algébrique composée d'un corps

Extension finie d'un corps. Soit $\mathscr{P}$ un sous-corps du corps $\mathscr{F}$. On peut alors considérer $\mathscr{F}$ comme un espace vectoriel sur $\mathscr{P}$, c'est-à-dire envisager l'espace vectoriel

$$\langle F, +, \{\omega_\lambda \mid \lambda \in P\}\rangle,$$

où ω_λ est une opération de multiplication des éléments de F par un scalaire $\lambda \in P$.

DÉFINITION. Une extension $\mathscr{F}$ du corps $\mathscr{P}$ est dite *finie* si $\mathscr{F}$, espace vectoriel sur $\mathscr{P}$, est de dimension finie. Cette extension est notée $[\mathscr{F} : \mathscr{P}]$.

PROPOSITION 3.1. *Si α est un élément algébrique de degré n sur $\mathscr{P}$, alors $[\mathscr{P}(\alpha) : \mathscr{P}] = n$.*

Cette proposition découle directement du théorème 2.5.

DÉFINITION. Une extension $\mathscr{F}$ du corps $\mathscr{P}$ est dite *algébrique* si chaque élément de F est algébrique sur $\mathscr{P}$.

THÉORÈME 3.2. *Toute extension finie $\mathscr{F}$ du corps $\mathscr{P}$ est algébrique sur $\mathscr{P}$.*

Démonstration. Soit n la dimension de $\mathscr{F}$ sur $\mathscr{P}$. Le théorème est apparemment vrai si $n = 0$. Posons que $n > 0$. Tous $n + 1$ éléments de F sont linéairement dépendants sur $\mathscr{P}$. En particulier, le système d'éléments $1, \alpha, \ldots, \alpha^n$ est linéairement dépendant, c'est-à-dire qu'il existe dans P des éléments $c_0, c_1, \ldots, c_n$ non tous nuls, tels que

$$c_0 \cdot 1 + c_{1\alpha} + \ldots + c_n\alpha^n = 0.$$

Par conséquent, l'élément α est algébrique sur $\mathscr{P}$. □

Remarquons qu'il existe des extensions algébriques du corps qui ne sont pas des extensions finies.

Extension algébrique composée d'un corps. Une extension $\mathcal{F}$ du corps $\mathcal{P}$ est dite composée s'il existe une chaîne ascendante de sous-corps $\mathcal{L}_i$ du corps $\mathcal{F}$, telle que

$$\mathcal{P} = \mathcal{L}_0 \dashv \mathcal{L}_1 \dashv \ldots \dashv \mathcal{L}_k = \mathcal{F} \text{ et } k > 1.$$

THÉORÈME 3.3. *Soient $\mathcal{F}$ une extension finie du corps $\mathcal{L}$ et $\mathcal{L}$ une extension finie du corps $\mathcal{P}$. Alors, $\mathcal{F}$ est une extension finie du corps $\mathcal{P}$ et*

(I) $[\mathcal{F} : \mathcal{P}] = [\mathcal{F} : \mathcal{L}] \cdot [\mathcal{L} : \mathcal{P}]$.

D é m o n s t r a t i o n. Soient

(1) $\alpha_1, \ldots, \alpha_m$

la base du corps $\mathcal{L}$ sur $\mathcal{P}$ (considéré comme un espace vectoriel) et

(2) $\beta_1, \ldots, \beta_n$

la base du corps $\mathcal{F}$ sur $\mathcal{L}$. Tout élément d de F peut être exprimé linéairement en fonction de la base:

(3) $d = l_1\beta_1 + \ldots + l_n\beta_n \qquad (l_k \in L)$.

Les coefficients l_k peuvent être exprimés linéairement en fonction de la base (1):

(4) $l_k = p_{1k}\alpha_1 + \ldots + p_{mk}\alpha_m \qquad (p_{ik} \in P)$.

En portant l'expression du coefficient l_k dans (3), il vient

$$d = \sum_{\substack{i \in \{1, \ldots, m\} \\ k \in \{1, \ldots, n\}}} p_{ik}\alpha_i\beta_k.$$

Ainsi, chaque élément du corps $\mathcal{F}$ est représentable sous forme d'une combinaison linéaire d'éléments de l'ensemble B, où

$$B = \{\alpha_i\beta_k \mid i \in \{1, \ldots, m\}, k \in \{i, \ldots, n\}\}.$$

Notons que l'ensemble B est composé de nm éléments.

Montrons que B est la base de $\mathcal{F}$ sur le corps $\mathcal{P}$. Il nous faut montrer que le système d'éléments de l'ensemble B est linéairement ndépendant. Soit

(5) $\sum_{i, k} c_{ik}\alpha_i\beta_k = 0$,

où $c_{ik} \in P$. Etant donné que le système (2) est linéairement indépendant sur $\mathcal{L}$, il s'ensuit de (5) l'égalité

(6) $c_{1k}\alpha_1 + \ldots + c_{mk}\alpha_m = 0 \qquad (k = 1, \ldots, n)$.

Les éléments $\alpha_1, \ldots, \alpha_m$ étant linéairement indépendants sur $\mathcal{P}$, il s'ensuit de (6) les égalités

$$c_{1k} = 0, \ldots, c_{mk} = 0 \qquad (k = 1, \ldots, n),$$

qui montrent que tous les coefficients dans (5) sont nuls. Ainsi, le système d'éléments de B est linéairement indépendant et est une base de $\mathcal{F}$ sur $\mathcal{P}$.

Bref, on a établi que $[\mathcal{F}, \mathcal{P}] = nm = [\mathcal{F} : \mathcal{L}] \cdot [\mathcal{F} : \mathcal{P}]$. Par conséquent, $\mathcal{F}$ est une extension finie du corps $\mathcal{P}$ et on a la formule (I). □

DÉFINITION. Une extension $\mathcal{F}$ du corps $\mathcal{P}$ est appelée *extension algébrique composée* s'il existe une chaîne ascendante de sous-corps du corps $\mathcal{F}$

$$\mathcal{P} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \ldots \subset \mathcal{L}_k = \mathcal{F} \qquad (k > 1) \tag{1}$$

telle que pour $i = 1, \ldots, k$ le corps $\mathcal{L}_i$ soit une extension algébrique simple du corps $\mathcal{L}_{i-1}$. Le nombre k est dit *longueur de la chaîne* (1).

COROLLAIRE 3.4. *Une extension algébrique composée $\mathcal{F}$ du corps $\mathcal{P}$ est une extension finie du corps $\mathcal{P}$.*

La démonstration s'effectue sans peine par récurrence sur la longueur de la chaîne (1) en s'appuyant sur le théorème 3.3.

THÉORÈME 3.5. *Soit $\alpha_1, \ldots, \alpha_k$ des éléments algébriques du corps $\mathcal{F}$ sur le corps $\mathcal{P}$. Alors le corps $\mathcal{P}(\alpha_1, \ldots, \alpha_k)$ est une extension finie du corps $\mathcal{P}$.*

D é m o n s t r a t i o n. Soit

$$\mathcal{L}_0 = \mathcal{P},\ \mathcal{L}_1 = \mathcal{P}[\alpha_1],\ \mathcal{L}_2 = \mathcal{P}[\alpha_1, \alpha_2], \ldots, \mathcal{L}_k = \mathcal{P}[\alpha_1, \ldots, \alpha_k].$$

Dans ce cas $\mathcal{L}_1 = \mathcal{P}[\alpha_1]$ est une extension algébrique simple du corps $\mathcal{L}_0$; $\mathcal{L}_2$ est une extension algébrique simple du corps $\mathcal{L}_1$, car

$$\mathcal{L}_2 = \mathcal{P}[\alpha_1, \alpha_2] = (\mathcal{P}[\alpha_1])[\alpha_2] = \mathcal{L}_1[\alpha_2] = \mathcal{L}_1(\alpha_2), \text{ etc.}$$

Ainsi,

$$\mathcal{P} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \ldots \subset \mathcal{L}_k = \mathcal{F},$$

où $\mathcal{L}_i = \mathcal{L}_{i-1}(\alpha_i)$ pour $i = 1, \ldots, k$, c'est-à-dire que chaque terme de la chaîne (2) est une extension algébrique simple du terme précédent de la chaîne. Bref, le corps $\mathcal{F}$ est une extension algébrique composée du corps $\mathcal{P}$. Par conséquent, en vertu du corollaire 3.4, le corps $\mathcal{F}$ est une extension finie du corps $\mathcal{P}$. □

COROLLAIRE 3.6. *Une extension algébrique composée d'un corps est une extension algébrique de ce corps.*

Simplicité de l'extension algébrique composée d'un corps.

THÉORÈME 3.7. *Supposons qu'un corps numérique $\mathcal{F}$ est une extension algébrique composée du corps $\mathcal{P}$. Alors $\mathcal{F}$ est une extension algébrique simple du corps $\mathcal{P}$.*

Démonstration. Soit $\mathcal{P} \dashv \mathcal{L} \dashv \mathcal{F}$, avec $L = P(\alpha)$, $F = L(\beta)$ et par conséquent,

$$F = P(\alpha, \beta).$$

Soient f et g des polynômes minimaux sur $\mathcal{P}$ respectivement pour les nombres α et β et $\deg f = m$, $\deg g = n$. Les polynômes f et g sont irréductibles sur $\mathcal{P}$ et, par conséquent, ne possèdent pas dans le corps $\mathcal{C}$ de nombres complexes des racines multiples. Soient

$\alpha = \alpha_1, \ldots, \alpha_m$ des racines du polynôme f dans **C** et

$\beta = \beta_1, \ldots, \beta_n$ des racines du polynôme g dans **C**.

Considérons l'ensemble fini M:

$$M = \left\{ \frac{\alpha_i - \alpha}{\beta - \beta_k} \mid i \in \{1, \ldots, m\}, \quad k \in \{2, \ldots, n\} \right\}.$$

Puisque $\mathcal{P}$ est un ensemble numérique (et, par suite, infini) il existe dans P un nombre c distinct des éléments de l'ensemble M $c \in P \setminus M$, $c \notin M$. Soit

(1) $\gamma = \alpha + c\beta$.

On a alors les relations

(2) $\gamma \neq \alpha_i + c\beta_k \qquad (i \in \{1, \ldots, m\}, \quad k \in \{2, \ldots, n\})$.

En effet, en cas d'égalité de $\alpha + c\beta = \alpha_i + c\beta_k$, on aurait

$$c = \frac{\alpha_i - \alpha}{\beta - \beta_k} \in M,$$

ce qui est contradictoire au choix du nombre c.

Soient $\mathcal{F}_1 = \mathcal{P}(\gamma)$ et $\mathcal{F}_1[x]$ un anneau des polynômes en x. Supposons que $h = f(\gamma - cx)$ est un polynôme de $F_1[x]$ $(\gamma, c \in P(\gamma) = F_1)$. Montrons que $x - \beta$ est le plus grand commun diviseur des polynômes h et g dans l'anneau $\mathcal{F}_1[x]$. Vu que $g(\beta) = 0$, $x - \beta$ divise g dans $\mathcal{C}[x]$. Ensuite, en vertu de (1)

$$h(\beta) = f(\gamma - c\beta) = f(\alpha) = 0.$$

Donc, $x - \beta$ divise le polynôme h dans $\mathcal{C}[x]$. Ainsi, $x - \beta$ est un diviseur commun de h et g dans l'anneau $\mathcal{C}[x]$.

Démontrons que g et h n'ont pas dans **C** de racines distinctes de β. En effet, posons que β_k, $k \in \{2, \ldots, n\}$ est leur racine commune. Alors, $h(\beta_k) = f(\gamma - c\beta_k) = 0$. Il se trouvera donc un tel indice $i \in \{1, \ldots, m\}$ pour lequel $\gamma = \alpha_i + c\beta_k$ $(k > 1)$, or c'est en contradiction avec (2). En s'appuyant sur ce qui précède on conclut que $x - \beta$ est le plus grand commun diviseur de g et h dans $\mathcal{C}[x]$.

Vu que $x - \beta$ est un polynôme normé, il s'ensuit que $x - \beta$ est le plus grand commun diviseur de g et h dans l'anneau $\mathscr{F}_1\,[x]$. Donc,

$$(x - \beta) \in F_1\,[x] \text{ et } \beta \in F_1 = P\,(\gamma).$$

De plus, $\alpha = \gamma - c\beta \in F_1$. Ainsi,

$$F = P\,(\alpha,\ \beta) \subset F_1, \qquad F_1 \subset F.$$

Donc, $F = P\,(\gamma)$. Vu que γ (comme d'ailleurs tout élément de F) est un élément algébrique sur $\mathscr{P}$ et $\mathscr{F} = \mathscr{P}\,(\gamma)$, on a $\mathscr{F} = \mathscr{P}\,(\gamma)$ qui est l'extension algébrique simple cherchée du corps $\mathscr{P}$. □

Corps des nombres algébriques. Dans la classe des sous-corps d'un corps des nombres complexes le corps des nombres algébriques est l'un des plus importants.

DÉFINITION. On appelle *nombre algébrique* un nombre complexe constituant une racine d'un polynôme de degré positif avec des coefficients rationnels.

Notons qu'un nombre algébrique est un nombre complexe quelconque algébrique sur le corps $\mathscr{Q}$. En particulier, tout nombre rationnel est algébrique.

THÉORÈME 3.8. *L'ensemble A de tous les nombres algébriques est fermé dans l'anneau $\mathscr{C} = \langle \mathrm{C},\ +,\ -,\ \cdot,\ 1\rangle$ des nombres complexes. L'algèbre $\mathscr{A} = \langle A,\ +,\ -,\ \cdot,\ 1\rangle$ est un corps, un sous-corps du corps $\mathscr{C}$.*

Démonstration. Soient a et b tous éléments de A. Selon le corollaire 3.6, le corps $\mathscr{Q}\,(a,\ b)$ est algébrique sur $\mathscr{Q}$. Aussi les nombres $a + b$, $-a$, ab, 1 sont-ils des nombres algébriques, c'est-à-dire appartiennent à l'ensemble A. L'ensemble A est ainsi fermé relativement aux opérations principales de l'anneau $\mathscr{C}$. L'algèbre $\mathscr{A}$ est donc un anneau comme sous-anneau de l'anneau $\mathscr{C}$.

En outre, si a est un élément non nul de A, on a $a^{-1} \in \mathrm{Q}\,(a,\ b)$ et, partant, appartient à A. Par conséquent, l'algèbre $\mathscr{A}$ est un corps, un sous-corps du corps $\mathscr{C}$. □

DÉFINITION. *Le corps $\mathscr{A} = \langle A,\ +,\ -,\ \cdot,\ 1\rangle$ est appelé corps des nombres algébriques.*

Fermeture algébrique d'un corps des nombres algébriques.

THÉORÈME 3.9. *Un corps des nombres algébriques est algébriquement fermé.*

Démonstration. Soit $\mathscr{A}\,[x]$ un anneau de polynômes en x sur le corps $\mathscr{A}$ des nombres algébriques. Soit

$$f = a_0 + a_1x + \ldots + a_nx^n \qquad (a_0,\ \ldots,\ a_n \in A)$$

un polynôme quelconque de degré positif de $A\,[x]$. Il nous faut démontrer que f admet une racine dans A. Vu que $f \in \mathrm{C}\,[x]$ et que le corps $\mathscr{C}$ est algébriquement fermé, f admet une racine dans $\mathscr{C}$, c'est-à-dire il existe un nombre complexe c tel que $f\,(c) = 0$. Soient $\mathscr{L} = \mathscr{Q}\,(a_0,\ \ldots,\ a_n)$ et $\mathscr{L}\,(c)$ une extension algébrique simple du corps $\mathscr{L}$ par adjonction de c. Alors, $\mathscr{Q} \dashv \mathscr{L} \dashv \mathscr{L}(c)$, $\mathscr{L}\,(c)$ étant l'extension finie du corps $\mathscr{L}$. En vertu du théorème 3.2, $\mathscr{L}$ est une

32—01762

extension finie du corps $\mathcal{Q}$. En vertu du théorème 3.3. $\mathcal{L}(c)$ est une extension finie du corps $\mathcal{Q}$. D'où, selon le théorème 3.2, le corps $\mathcal{L}(c)$ est donc une extension algébrique du corps $\mathcal{Q}$ et, par suite, $c \in A$. Ainsi, tout polynôme de $A[x]$ de degré positif admet dans A une racine, c'est-à-dire le corps $\mathcal{A}$ est algébriquement fermé. □

Exercices

1. Chercher le degré du corps $\mathcal{F}$ sur le corps $\mathcal{P}$ si

(a) $\mathcal{F} = \mathcal{Q}(\sqrt{2}, \sqrt{3})$, $\mathcal{P} = \mathcal{Q}$; (b) $\mathcal{F} = \mathcal{Q}(\sqrt{2}, \sqrt[3]{5})$, $\mathcal{P} = \mathcal{Q}(\sqrt{2})$; (c) $\mathcal{F} = \mathcal{R}$, $\mathcal{P} = \mathcal{R}$.

2. Chercher la base et le degré du corps $\mathcal{F}$ sur le corps $\mathcal{P}$ si

(a) $\mathcal{F} = \mathcal{Q}(i, \sqrt[3]{2})$, $\mathcal{P} = \mathcal{Q}$; (b) $\mathcal{F} = \mathcal{R}(-i)$, $\mathcal{P} = \mathcal{R}$; (c) $\mathcal{F} = \mathcal{C}$, $\mathcal{P} = \mathcal{C}$.

3. Soient f et g des polynômes sur le corps des nombres rationnels admettant une racine réelle commune. Démontrer que f et g possèdent un diviseur commun de puissance positive avec coefficients rationnels.

4. Démontrer qu'un polynôme irréductible sur un corps numérique n'admet pas de racines multiples dans un corps des nombres complexes.

5. Démontrer qu'un nombre complexe est un nombre algébrique si et seulement s'il est une racine d'un polynôme de degré positif avec coefficients entiers.

§ 4. Conditions de résolubilité d'une équation de troisième degré par radicaux carrés

Notion de résolubilité d'une équation par radicaux carrés.

DÉFINITION. Un corps $\mathcal{F}$ est dit *extension quadratique du corps* $\mathcal{P}$ s'il existe un élément α tel que $F = P(\alpha)$, $\alpha \notin P$, $\alpha^2 \in P$.

Exemples. 1. Le corps $\mathcal{Q}(2^{1/2})$ est une extension quadratique du corps $\mathcal{Q}$.

2. Le corps $\mathcal{R}(i)$ est une extension quadratique du corps $\mathcal{R}$.

3. Le corps $\mathcal{Q}(2^{1/3})$ n'est pas une extension quadratique de $\mathcal{Q}$.

On dit que l'équation

$$(1) \quad x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0 \qquad (a_i \in Q)$$

est résoluble par radicaux carrés si ses racines peuvent être exprimées de façon rationnelle (c'est-à-dire à l'aide des opérations d'addition, de soustraction, de multiplication et de division) par des racines d'une chaîne d'équations quadratiques binomiales:

$$\begin{aligned}
&x^2 - \alpha_0 = 0, \qquad \alpha_0 \in Q = F_0;\\
&x^2 - \alpha_1 = 0, \qquad \alpha_1 \in F_1 = F_0(\sqrt{\alpha_0});\\
&x^2 - \alpha_2 = 0, \qquad \alpha_2 \in F_2 = F_1(\sqrt{\alpha_1});\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&x^2 - \alpha_{k-1} = 0, \qquad \alpha_{k-1} \in F_{k-1} = F_{k-2}(\sqrt{\alpha_{k-2}}).
\end{aligned}$$

Ainsi, toutes les racines de l'équation (1) s'expriment de façon rationnelle par les nombres $\sqrt{\alpha_0}$, $\sqrt{\alpha_1}$, . . ., $\sqrt{\alpha_{k-1}}$ et appartiennent au corps $\mathcal{F}_k = \mathcal{F}_{k-1}(\sqrt{\alpha_{k-1}})$.

En d'autres termes, l'équation (1) est résoluble par des radicaux carrés s'il existe une chaîne ascendante des corps numériques

$$\mathbb{Q} = \mathcal{F}_0 \subset \mathcal{F}_1 \subset \ldots \subset \mathcal{F}_{k-1} \subset \mathcal{F}_k$$

telle que chaque corps $\mathcal{F}_i$ de la chaîne soit une extension quadratique du corps précédent $\mathcal{F}_{i-1}$, le corps $\mathcal{F}_k$ contenant toutes les racines de l'équation (1).

DÉFINITION. On dit que l'équation (1) *est résoluble par radicaux* si ses racines peuvent être exprimées de façon rationnelle par des racines d'une chaîne d'équations binomiales:

$$x^{n_0} - \alpha_0 = 0, \qquad \alpha \in \mathbb{Q} = F_0;$$
$$x^{n_1} - \alpha_1 = 0, \qquad \alpha_1 \in F_1 = F_0(\sqrt[n_0]{\alpha_0});$$
$$x^{n_2} - \alpha_2 = 0, \qquad \alpha_2 \in F_2 = F_1(\sqrt[n_1]{\alpha_1});$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x^{n_{k-1}} - \alpha_{k-1} = 0, \qquad \alpha_{k-1} \in F_{k-1} = F_{k-2}(\sqrt[n_{k-2}]{\alpha_{k-2}}).$$

Ainsi, toutes les racines de l'équation (1) s'expriment de façon rationnelle par les nombres $\sqrt[n_0]{\alpha_0}$, . . ., $\sqrt[n_{k-1}]{\alpha_{k-1}}$ et appartiennent au corps $\mathcal{F}_k = \mathcal{F}_{k-1}(\sqrt[n_{k-1}]{\alpha_{k-1}})$.

Conditions de résolubilité d'une équation de troisième degré par radicaux carrés.

THÉORÈME 4.1. *Une équation du troisième degré*

(1) $x^3 + ax^2 + bx + c = 0$

à coefficients rationnels est résoluble par radicaux carrés si et seulement si elle admet au moins une racine rationnelle.

Démonstration. Si le polynôme $f = x^3 + ax^2 + bx + c$ admet au moins une racine rationnelle, par exemple d, ce polynôme peut alors se représenter sous forme

$$f = (x - d)(x^2 + ex + g),$$

où $e, g \in \mathbb{Q}$. L'équation (1) est donc résoluble par radicaux carrés.

Supposons que l'équation (1) est résoluble par radicaux carrés tout en n'admettant pas de racines rationnelles. Il existe alors une chaîne d'extensions quadratiques

(2) $\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_{k-1} \subset F_k$,

telle qu'au moins une des racines x_1, x_2, x_3 de l'équation (1) soit contenue dans $F_k \setminus F_{k-1}$, par exemple

(3) $x_1 \in F_k \setminus F_{k-1}$,

et aucune des racines x_1, x_2, x_3 de l'équation (1) n'est contenue dans F_{k-1},

(4) $\{x_1, x_2, x_3\} \cap F_{k-1} = \varnothing$.

Le corps $\mathcal{F}_k$ est une extension quadratique du corps F_{k-1}, c'est-à-dire qu'il existe un élément $\alpha \in F_k \setminus F_{k-1}$ tel que

(5) $F_k = F_{k-1}(\alpha), \quad \alpha \notin F_{k-1}, \quad \alpha^2 \in F_{k-1}$.

Sur la base de (3) et (5), on conclut que

(6) $x_1 = p + q\alpha$, où $p, q \in F_{k-1}, \qquad q \neq 0$.

Une vérification directe montre que $p - q\alpha$ est également une racine du polynôme f. En effet,

(7) $$f(p + q\alpha) = (p + q\alpha)^3 + a(p + q\alpha)^2 + \\ + b(p + q\alpha) + c = A + B\alpha,$$

où

(8) $$A = f(p) + 3pq^2\alpha^2 + aq^2\alpha^2, \\ B = 3p^2q + q^3\alpha^2 + 2apq + bq.$$

Etant donné que $A, B \in F_{k-1}$ et $\alpha \notin F_{k-1}$, il s'ensuit de

(9) $f(p + q\alpha) = A + B\alpha = 0$

que

(10) $A = B = 0$.

Sur la base de (7), (8), (9) et (10), on conclut que

$$f(p - q\alpha) = A - B\alpha = 0.$$

Ainsi, $p - q\alpha$ est également une racine du polynôme f. Soit $x_2 = p - q\alpha$. Alors, en vertu de (6), $x_1 - x_2 = 2q\alpha \neq 0$ et, par suite, $x_1 \neq x_2$.

Selon les formules de Viète, $x_1 + x_2 + x_3 = -a$. En outre, en vertu de (6), $x_1 + x_2 = 2p \in F_{k-1}$. Donc, $x_3 = -a - 2p \in F_{k-1}$, ce qui est en contradiction avec la proposition (4). □

COROLLAIRE 4.2. *L'équation* (1) *avec coefficients rationnels est résoluble par radicaux carrés si et seulement si le polynôme* $x^3 + ax^2 + bx + c$ *est irréductible dans l'anneau* $\mathbb{Q}[x]$.

Exemples de problèmes irrésolubles par radicaux carrés. On démontre en géométrie que les racines de l'équation $x^3 + ax^2 + bx + c = 0$ avec coefficients rationnels peuvent être construites au compas et à la règle si et seulement si cette équation est résoluble par radicaux

carrés, c'est-à-dire si la solution de cette équation se réduit à celle d'une chaîne d'équations quadratiques.

Problème de doublage d'un cube. *Construire l'arête d'un cube dont le volume est double de celui du cube donné.*

On ne dispose que d'un segment: l'arête du cube donné; posons que ce segment est un segment unité. Alors, la longueur x de l'arête du cube cherché vérifie l'équation

$$(1) \quad x^3 - 2 = 0.$$

Cette équation est irrésoluble par radicaux carrés, car elle ne possède pas de racines rationnelles. Donc, *les racines de l'équation* (1) *ne peuvent être construites au compas et à la règle.*

Problème de trisection d'un angle. *Diviser l'angle donné en trois parties égales.*

On peut imaginer deux rayons d'origine O formant un angle φ. Traçons un arc de cercle de rayon unité. Construisons le point A de manière que le segment OA ait une longueur $a = \cos\varphi$. Réciproquement: connaissant le segment OA de longueur $\cos\varphi$ il est facile de construire l'angle au moyen du compas et de la règle. On peut donc considérer que c'est l'angle $x = \cos\frac{\varphi}{3}$ qui est cherché. Comme

$$\cos\varphi + i\sin\varphi = \left(\cos\frac{\varphi}{3} + i\sin\frac{\varphi}{3}\right)^3 =$$

$$= \cos^3\frac{\varphi}{3} - 3\cos\frac{\varphi}{3}\sin^2\frac{\varphi}{3} + i\left(3\cos^2\frac{\varphi}{3}\sin\frac{\varphi}{3} - \sin^3\frac{\varphi}{3}\right),$$

on a

$$\cos\varphi = \cos^3\frac{\varphi}{3} - 3\cos\frac{\varphi}{3}\sin^2\frac{\varphi}{3} =$$

$$= \cos^3\frac{\varphi}{3} - 3\cos\frac{\varphi}{3}\left(1 - \cos^2\frac{\varphi}{3}\right)$$

et

$$4\cos^3\frac{\varphi}{3} - 3\cos\frac{\varphi}{3} - \cos\varphi = 0.$$

Puisque $x = \cos\frac{\varphi}{3}$, on a

$$(1) \quad 4x^3 - 3x - a = 0.$$

Pour $\varphi = \frac{\pi}{2}$, $a = 0$ et, partant, l'équation (1) est résoluble par radicaux carrés.

Mais si $\varphi = \frac{\pi}{3}$, $a = \cos\frac{\pi}{3} = \frac{1}{2}$, et l'on obtient l'équation

$$(2) \quad 8x^3 - 6x - 1 = 0.$$

En y posant $y = 2x$, il vient

(3) $y^3 - 3y - 1 = 0.$

L'équation (3) et, partant, (2) est irrésoluble par radicaux carrés, car elle n'a pas de racines rationnelles. Par conséquent, les racines de ces équations ne peuvent être construites au compas et à la règle. *Ainsi, la trisection de l'angle $\pi/3$ au compas et à la règle est impossible.*

Problème de construction d'un heptagone régulier. *Construire un heptagone régulier inscrit dans un cercle unité.*

Les racines de l'équation $z^7 - 1 = 0$ sont représentées par des sommets d'un heptagone régulier inscrit dans un cercle unité. Une des racines de cette équation vaut l'unité, quant aux autres, elles vérifient l'équation

(1) $z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0.$

Démontrons que l'équation (1) est irrésoluble par radicaux carrés. En divisant les deux membres de l'équation (1) par z^3 et en groupant les termes, on obtient

$$\left(z+\frac{1}{z}\right)^3 - 3\left(z+\frac{1}{z}\right) + \left(z+\frac{1}{z}\right)^2 + \left(z+\frac{1}{z}\right) - 1 = 0.$$

En posant

(2) $t = z + \frac{1}{z}$,

il vient

(3) $t^3 + t^2 - 2t - 1 = 0.$

L'équation (3) est irrésoluble par radicaux carrés, car elle n'a pas de racines rationnelles. L'équation (1) est donc irrésoluble par radicaux carrés. En effet, si l'équation (1) était résoluble par radicaux carrés, alors, en vertu de (2), l'équation (3) serait aussi résoluble par radicaux carrés. Par conséquent, les racines de l'équation (1) ne peuvent être construites au compas et à la règle. Il s'ensuit qu'*on ne peut construire un heptagone régulier au compas et à la règle.*

Pour quels n naturels ($n > 2$) peut-on construire un polygone régulier à n angles en se servant du compas et de la règle?

Ce problème a été complètement résolu par Gauss en 1796. Gauss a démontré que la construction n'est possible que dans le cas où n peut se représenter sous forme

$$n = 2^k p_1 p_2 \ldots p_m,$$

où k est un nombre naturel et $p_1, \ldots, p_m$ sont des nombres premiers différents de la forme $2^m + 1$ ($m \in N \setminus \{0\}$).

Exercices

1. Montrer que le polynôme $x^6 + x^3 + 1$ est irréductible sur le corps des nombres rationnels.

2. Montrer qu'un polynôme de troisième degré sur un corps est soit irréductible soit admet une racine dans ce corps. Le polynôme $x^5 - 5x^3 + 1$ est-il irréductible sur le corps des nombres rationnels?

3. Montrer que le polynôme à deux variables $x^2 + y^2 - 1$ est irréductible sur le corps des nombres rationnels. Est-il réductible sur le corps des nombres complexes?

4. Démontrer que l'équation $x^5 - 1 = 0$ est résoluble par radicaux carrés.

5. Démontrer qu'un pentagone régulier peut être construit au compas et à la règle.

6. Démontrer qu'un ennéagone régulier ne peut être construit au compas et à la règle.

BIBLIOGRAPHIE

1. И. В. Арнольд. Теория чисел. М., 1939.
2. А. А. Бухштаб. Теория чисел. М., 1966.
3. И. М. Виноградов. Основы теории чисел. М., 1976.
4. Б. Л. Ван-дер-Варден. Алгебра. М., 1976.
5. И. М. Гельфанд. Лекции по линейной алгебре. М., 1966.
6. Л. А. Калужнин. Введение в общую алгебру. М., 1973.
7. М. И. Каргаполов, Ю. И. Мерзляков. Основы теории групп. М., 1972.
8. А. И. Кострикин. Введение в алгебру. М., 1977.
9. А. Г. Курош. Курс высшей алгебры. М., 1971. (Kurosh A. Cours d'algèbre supérieure. Editions Mir, 1973).
10. А. Г. Курош. Лекции по общей алгебре. М., 1962.
11. И. А. Лавров, Л. Л. Максимова. Задачи по теории множеств, математической логике и теории алгоритмов. М., 1975.
12. А. И. Мальцев. Основы линейной алгебры. М., 1970.
13. А. И. Мальцев. Алгебраические системы. М., 1970.
14. А. А. Марков. Теория алгоритмов.— Труды Математического института АН СССР 42, 1954.
15. Э. Мендельсон. Введение в математическую логику. М., 1971.
16. П. С. Новиков. Элементы математической логики. М., 1973.
17. М. М. Постников. Теория Галуа. М., 1963.
18. И. В. Проскуряков. Сборник задач по линейной алгебре. М., 1967.
19. Е. Слупецкий, Л. Борковский. Элементы математической логики и теории множеств. М., 1965.
20. Р. Р. Столл. Множества, логика, аксиоматические теории. М., 1968.
21. Д. К. Фаддеев, И. С. Соминский. Сборник задач по высшей алгебре. М., 1977.
22. С. Феферман. Числовые системы. М., 1971.
23. Dieudonné J. Algèbre linéaire et géométrie élémentaire. Paris, 1968.
24. Faure R., Kaufmann A., Denis-Papin M. Mathématiques nouvelles. Paris, 1964.
25. Gale D. The Theory of Linear Economic Models, N.Y., 1960.
26. Halmoss P. Finite-dimensional vector spaces. 2nd ed. Princeton.
27. Hall M. jr. Combinatorial Theory. Toronto, 1967.
28. Hasse H. Zahlentheorie. Berlin, 1950.

INDEX

TABLE DES MATIÈRES

